PERFORMANCE WORK STATEMENT (PWS)
For
DEFENSE HEALTH AGENCY (DHA)
TIER 2.5 HELPDESK SUPPORT AND DATA RECONCILIATION
GSA TASK ORDER #ID03160001
Revised per Modification 001

1.0 Background:

On October 1, 2013, the Department of Defense established the Defense Health Agency (DHA) to manage the activities of the Military Heath System. These activities were previously managed by Tricare Management Activity (TMA). The new program office eliminates organizational redundancies, streamlines operations and enhances the delivery of much needed information technology solutions to all Military Health System (MHS) beneficiaries. The combined programs advance efforts to document seamlessly and electronically the health care provided by military authorized providers to all Army, Navy, Air Force, and Marine Corps personnel, retirees and their families. DHA is committed to delivering clinical IT solutions that enable quality continuity of care and timely administration of benefits. DHA's primary focus is on enhancing usability of the military's Electronic Health Record (EHR) by improving system speed, reliability, data quality, and usability (look and feel) of the product to better meet the needs of the military's medical community.

The use of the Essentris Inpatient Documentation Solution eliminates the majority of paper based inpatient documentation by providing real time documentation into various software modules. The use of Essentris across Medical Treatment Facilities (MTF) s allows for standardization of processes and sharing of documentation across the Department of Defense.

ESSENTRIS: Essentris, a Commercial Off -the Shelf (COTS) product, is a mission-critical comprehensive clinical documentation system for use in Services' treatment facilities since 1988. CIS is a state of the art system with the following key components: a) patient chart that includes flow sheets, treatment notes, medication administration, care plans and integrated order entry, b) automated collection and charting of physiologic data from monitors, and c) real-time reporting and analytics.

Sustainment: The Military Health System's inpatient documentation solution, CIS, is a comprehensive clinical documentation system for use in acute care hospitals. It captures point-of-care data from physiological devices, fetal/uterine devices, ventilators and other patient care machines at the patient's bedside. All clinical documentation is created and stored in the CIS. This clinical data may be aggregated, trended, and analyzed to manage care for a single patient or for an entire patient population. The key interfaces are:

- Composite Healthcare System (CHCS)
- Bi-directional Health Information Exchange (BHIE)
- jXP (formerly known as iXP or Intersystem Trans(X) lation Protocol)
- Interface from CHCS to Essentris (ICE)
- Interface to Computrition
- Interface to SmartSuite

The system is currently deployed in Air Force, Navy, Army and NCR MD CIS sites. As a deployed application, Essentris is in a sustainment mode at 57 sites and requires hardware and software maintenance. Additionally, as a deployed automated information system, Essentris requires periodic information assurance evaluations.

Composite Health Care System (CHCS): The CHCS is one of the most broadly deployed medical information systems in the world and it serves as the core medical information system for the DoD. Regardless of where military health care providers are assigned around the world, they have the same medical information system available to them facilitating the delivery of quality patient care to 9.1 million TRICARE beneficiaries. In 2004, CHCS was used to support more than 30 million appointments, 55 million prescriptions, 43 million laboratory tests, and 5 million radiology procedures.

CHCS continues to be one of the most broadly used Computerized Provider Order Entry (CPOE) systems in the Nation. This powerful system enables DoD providers to electronically order laboratory tests, retrieve test results, authorize radiology procedures and prescribe medications. Reducing the risk of illegible orders and completing drug interaction and appropriateness checks, the CPOE functionality of CHCS continues to safeguard care provided to our MHS beneficiaries. For patients, CHCS facilitates improvements in the delivery of health care that reduce wait time, increase access to medical and professional resources, and expedite diagnostic testing. For providers, CHCS promotes increased communication and supports near real-time access to local patient information.

Functional capabilities include patient registration, admission, disposition, and transfer; outpatient administration data; appointment scheduling; laboratory data; drug interaction alerts; quality assurance, radiology results; clinical dietetic administration; pharmacy alerts; computerized order entry and results retrieval; ad hoc reporting; and managed care.

Essentris interfaces to CHCS to acquire laboratory results, admissions/transfer and discharge information, and radiology results. This interface is a one-way interface from CHCS to Essentris. CHCS can be collocated at an MTF or remote/regionalized, where it can service multiple MTFs.

CHCS shares secure, encrypted data electronically with commercial reference laboratories and Department of Veterans Affairs (VA) facilities, and interfaces with more than 40 other clinical and administrative systems. Systems CHCS interfaces with include: the VA Consolidated Mail Outpatient Pharmacy system; TRICARE Online; Pharmacy Data Transaction Service; Defense Medical Logistics Standard Support program; Third Party Outpatient Collection System; Defense Blood Standard System; and the Defense Enrollment Eligibility Reporting System.

Armed Forces Health Longitudinal Technology Application (AHLTA): AHLTA is one of the world's largest clinical information systems, providing secure, 24/7 access to TRICARE beneficiaries' medical records worldwide. AHLTA is a key enabler of military medical readiness, and the centerpiece of the Military Health System's (MHS) electronic health record (EHR). Currently deployed on a global scale, AHLTA supports Force Health Protection (FHP) for DoD service members while serving abroad as well as health services provided to their family members and other beneficiaries in military medical facilities "back home." AHLTA data is stored in a central location to ensure health care providers have ready access to medical information when and where needed, to support the military's highly-mobile patient population. As military members move from location to location, AHLTA ensures information is readily available to support their health care needs. AHLTA also supports uniform, high-quality health promotion (i.e., population health, wellness, and disease management), and health care delivery to TRICARE beneficiaries across the DoD enterprise. This support will allow the MHS to track clinical care and exposures of deployed units, monitor demand-management effectiveness, better understand disease

prevalence and prevention, as well as study both clinical and management outcomes. AHLTA will also support the readiness mission of military forces with seamless communication capabilities back to the sustaining base. AHLTA is configured to meet the DoD's specialized requirements for delivery of care in environments that span from the forward deployed medic to the largest medical centers. Implementing a single solution used in all care environments ensures a complete medical record, including data from the theater of operations, is compatible with the DoD Command and Control system giving Commanders a clear view of what is going on medically in the field. In its current state, AHLTA leverages applications such as the legacy CHCS to perform routine patient appointment processes and scheduling, order laboratory tests, retrieve test results, authorize radiology procedures, and prescribe medications.

Bi-directional Health Information Exchange (BHIE): Essentris interfaces with the Department of Veterans Affairs (VA) BHIE Framework to send read-only in-patient discharge summaries to the VA and all notes to the SHARE presentation layer for DOD users in support of joint VA & DOD Sharing Initiatives. This interface may be internal to the MTF or external, depending on the location of the interfacing CHCS system. The Tomcat implementation on the Essentris servers allows CIS-Essentris to interface with the Department of Veterans Affairs (VA) BHIE Framework, in support of joint VA & DOD Sharing Initiatives, to send read-only in-patient discharge summaries and other pre-designated notes.

jXP (formerly known as iXP or Intersystem Trans(X) lation Protocol): Essentris, supports receiving HL7 Admission, Discharge, and Transfer messages (ADTs), Master File Notifications (MFNs), Order messages (ORMs), Order Result messages (ORUs), and Scheduling messages (SCHs) from CHCS. Additionally, Essentris transmits HL7 order messages to jXP for transmission to the CHCS Data Server. This is only implemented at Tripler Army Medical Center.

Interface from CHCS to Essentris (ICE): Essentris interfaces with CHCS to receive clinical and demographic information in an HL7 format. The ICE messages are triggered by the arrival of an ED or In-Patient encounter.

Interface to Computrition: Essentris interfaces with Computrition to send ADT and Order information to support the Nutritional ancillary department needs.

Interface to SmartSuite: Essentris interfaces with SmartSuite to send ADT, database items, medication and fluid orders, and fluid deliveries. SmartSuite uses icons to display details about a patient's condition outside of his/her hospital room.

1.1 Scope

The scope of this task order is to provide program-level Help Desk support to include evaluating, processing or resolving and tracking 100% of the Trouble Tickets identified for the Defense Health Clinical System (DHCS) Tier 2.5. This includes program management, detailed trend analysis and reporting, which must provide the DHCS with the ability to understand the state and performance of the DHCS Tier 2.5 triage and resolution functions.

1.2 Objective

The objective of this acquisition is to ensure that appropriate and timely action is taken to resolve any issues affecting the Armed Forces Health Longitudinal Technology Application (AHLTA) and CHCS users or system performance as the issues are elevated from the MHS Help Desk Tier 2.5 organization. The volume of Triaged Trouble Tickets is subject to increases and decreases in volume based on the activities and requirements of the Services, other contractor vendors, and by other means.

TASK ORDER REQUIREMENTS

1.3 Helpdesk and Technical Support Tasks and Deliverables

1.3.1 TIER 2.5 Triage Policy – Deliverable 27

The Tier 2.5 helpdesk Contractor shall validate and resolve each Trouble Ticket elevated for DHCS Tier III action. This includes all activities necessary to verify and analyze the issue for processing. The ticket will be elevated to the Tier III helpdesk for resolution if it cannot be resolved by the Tier 2.5 helpdesk. The Contractor shall define an effective **DHCS Tier III Triage Policy** to ensure quality and timely support **(Deliverable 27)**.

1.3.2 TIER 2.5 Process – Deliverable 28

The Contractor shall define, document, and implement processes and procedures for the DHCS Tier 2.5 Trouble Ticket Resolution capability. This includes process maps/flows, roles and responsibilities, inputs and outputs, templates, guides, checklits, etc. The processes must be used to ensure a repeatable flow of work activities, with a predictable outcome (**Deliverable 28).**

1.3.3 Verify Incoming Trouble Tickets

The Contractor shall review each Trouble Ticket to ensure that the documented information is complete, accurate, and sufficient to facilitate analysis of the issue. If necessary, the Contractor shall coordinate with the DHA Global Service Center/or ticket originator to confirm or obtain additional information.

1.3.4 Analyze Verified Trouble Tickets

The Contractor shall analyze each verified Trouble Ticket and assign a classification, priority, and severity to facilitate timely and appropriate processing of the issue. In an effort to more efficiently manage Trouble Ticket processing and subsequent resolution, the Contractor shall provide a mechanism to group submitted Trouble Tickets by similar system function or problem/failure type in order to identify those addressing identical issues.

In addition, any ticket identified as having potential patient safety consequences must be immediately elevated to the task manager or the designated POC for evaluation. Patient Safety tickets will also be sent the SDD Patient Safety Officer and SDD Engineering following notification of the TM or POC for immediate evaluation.

1.3.5 Process Trouble Tickets

The Contractor shall process each Trouble Ticket for resolution based upon the classification scheme as follows:

- Action Item – The Contractor shall resolve each Tier 2.5Trouble Ticket classified as an Action Item including data configurations, data transfers, data problems, access changes, 3M Health Data Dictionary issues etc.

- Configuration Issue – The Contractor shall process each Tier 2.5 Trouble Ticket classified as a Configuration Issue. This includes determining which operational support organization is responsible for resolving the issue (e.g., I&O, DISA, site, etc.) and transmitting the appropriate information.

- Software Defect – The Contractor shall process each Tier 2.5 Trouble Ticket classified as a Software Defect.

- Software Enhancement – The Contractor shall process each Tier 2.5 Trouble Ticket classified as a Software Enhancement. This includes submitting the Trouble Ticket and the supporting analysis information to the DHCS Product Manager for review.

- Provider Tickets – The contractor shall resolve Tier 2.5 Trouble Tickets submitted to correct provider account issues that include account not accessible, account not crossing, password issues, clinics not displaying, duplicate accounts, unmerging accounts, correcting CAC-related errors (1029 errors, Error Codes 32 & 91), unmerging CAC accounts, resetting CAC passwords, enabling access to AHLTA Web Print Folder or Role Modification, unlocking AHLTA Web Print accounts, clearing new results, and errors preventing a provider from signing an encounter.

- Ensure Local Cache Servers (LCS's) data coordinates with updates made to CDR data for tickets involving data transfers, such as unmerge actions and provider account settings.

1.3.6 Conduct Tier 2.5 Trouble Ticket Tracking and Performance Management

The Contractor shall provide the SDD with objective data to monitor and measure performance of the Tier 2.5 Trouble Ticket Resolution capability.

1.3.6.1 Trouble Ticket Tracking

The Contractor shall track the status of every Tier 2.5 Trouble Ticket upon submission, through remediation or development, testing, and implementation. The Contractor shall maintain the Trouble Ticket database(s), updating the Trouble Ticket information with any changes resulting from a SDD support entity. The Contractor shall maintain communication with the Trouble Ticket originator, providing status updates through closure.

1.3.7 Monthly Performance Reporting

The Contractor shall provide monthly metrics on the overall status and performance of the AHLTA and CHCS Tier 2.5 Trouble Ticket Resolution capability. The Contractor shall work collaboratively with the DHCS to define the final comprehensive measurement and analysis function. This work shall be reflected in a Decision Matrix **(Deliverable 31).** The Contractor shall generate a Risk Register; this document will act as a central repository for all risks identified by the organization and, for each risk, includes information such as source, nature, treatment option, existing counter-measures and recommended counter-measures **(Deliverable 32).**

Potential measurement data includes:

- Total Trouble Tickets submitted per month by severity and classification category,
- Total Trouble Tickets unresolved per month by severity and classification category,
- Total Trouble Tickets submitted for DT&E verification per month by severity and classification category,
- Total Trouble Tickets accepted by DT&E by severity and classification category,
- Total Trouble Tickets closed per month by severity and classification category,
- Total severity 1 & 2 software defects identified per build,
- Severity 1 & 2 trouble tickets resolution time trend,
- Number of trouble tickets in Deferred Status within 2 weeks,
- Average time to close trouble tickets by classification category, and
- Top Ten Action Items per month.

1.3.8 MHS Help Desk Database Support

The Contractor shall remain the primary point of contact for all trouble tickets elevated to DHCS Tier 2.5, ensuring that the DHA Global Service Center database is accurate and up-to-date. The Contractor shall receive; update, track, and close MHS trouble tickets using the current DHA Global Service Center Database. Access to the DHA Global Service Center Database shall be provided to the Contractor at no cost. The Contractor shall proactively and routinely collaborate with the DHA Global Service Center personnel to ensure tickets are resolved in an effective and efficient manner

1.3.8.1 MHS Incident Management Tool Support– Remedy

The Government furnished MHS Incident Management Tool of Choice (Remedy) is the only trouble ticket management tool used to enter, work, record status updates, and resolve MHS application and system incidents (also called trouble tickets) to include comprehensively documenting all resolution efforts and dispositions, including workarounds.

1.3.10 Deployment Support

The Contractor shall support the SDD deployment services where required in support of the Tier 2.5 process

1.3.11 Theater Data Reconciliation Support

1.3.11.1 Update Theater Data Reconciliation Users Guide – Deliverable 29

The Contractor shall update the Theater Data Reconciliation Users Guide that identifies the types of errors encountered and documents the reconciliation activities and steps required. This guide shall document the policy decisions and business rules for reconciling theater data encounter errors. The Theater Data Reconciliation Users Guide shall include the information required to be able to execute data reconciliation activities for theater encounters to the CDR (**Deliverable 29**).

1.3.11.2 Conduct Theater Data Reconciliation Activities – Deliverable 30

The Contractor shall conduct theater data reconciliation activities in accordance with the approved plan. This shall include resolution of the particular theater encounters residing in the theater data error logs so that the encounters may be ingested into the CDR. The Contractor working with the Integrator shall resubmit the resolved encounters so that the encounters are ingested into the CDR. This shall also include errors that are accumulating during the period of performance. The Contractor shall conduct root cause analysis, develop and implement reconciliation solutions to include the recommended policy and business rule changes to handle the particular instance automatically in the future. The Contractor shall provide the resultant findings and recommended policy/business rule changes. The Contractor shall propose a series of metrics and reports (**Deliverable 30**) that show the progress of the reconciliation and root cause activities. The Contractor shall provide these reports to the Government on a weekly basis.

1.3.11.3 Other Data Quality Issues

The Contractor shall analyze and resolve other Garrison and Theater data quality issues.

1.4 Optional Technical Support Task

The Government will exercise the optional task via a task order modification.

1.4.1 Data Quality Support Subject Matter Expert (Optional Task)

This is an optional task that may be exercised at the Government's discretion.

The Contractor shall perform tasks that identify and correct data quality issues in CHCS, AHLTA and the CDR.

- Provide services to identify, analyze, recommend, develop and implement enterprise technical solutions that will reduce and/or eliminate current patient registration errors, duplicate patients, and configuration control processes.

- Correct Patient Files. Review all records for accuracy and completeness. Focus efforts on the most important error type and most recent patient records within AHLTA/DEERS/Composite Healthcare System (CHCS). Resolve, correct, or complete missing information for the following types of patient record errors:
    - Potential duplicate AHLTA/CHCS/DEERS patient records
    - Pseudo Social Security Numbers (SSN)
    - Electronic Design Interchange Patient Number (EDI-PN)
    - Sponsor Name
    - Family Member Prefix (FMP)
    - Patient/Sponsor SSN
    - Patient Category (PATCAT)
    - Date of Birth (DOB)
    - Gender

- Correct National Enrollment Database (NED) Patient/Primary Care Information Transfer (PIT) discrepancies at MTFs not supported by any other contract that performs that service.

- Correct duplicate records within CHCS. Communicate with MTF Points of Contact on unresolved duplicate patients and registration errors. Follow-up with MTFs to ensure resolution.

- Ensure all patient file related information in CHCS is consistent with Department of Defense (DoD), Defense Health Agency (DHA) and DEERS directives.

- Analyze and resolve other related data quality issues.

2.1 Program Management Tasks and Deliverables

2.1.1 Government Oversight of the Task Order: Contracting Officer's Representative (COR)

The COR for the task order is a Government official who has been delegated specific technical, functional and oversight responsibilities for this task order. The COR is identified in the COR appointment letter, issued by the Contracting Officer, and will serve as the Government's primary technical point of contact for all task order activities and issues. The COR will oversee the task order on a day-to-day basis, will review Contractor performance and deliverables, and will receive and review all Contractor invoices.

2.1.2 Contractor Management of the Task Order: Task Manager (TM)

The Contractor shall provide sufficient management to ensure that this task is performed efficiently, accurately, on time, and in compliance with the requirements of this document. Specifically, the Contractor shall designate a single manager to oversee this task and supervise staff assigned to this task. The Contractor shall ensure that a Monthly Progress Report is submitted outlining the expenditures, billings, progress, status, and any problems/ issues encountered in the performance of this task.

2.1.2.1 Program Management Plan

The Contractor shall develop a Program Management Plan **(Deliverable 7)** that shall require Government approval. Following Government approval of the plan, it shall be applied by the Contractor to manage, track and evaluate the Contract performance. The Program Management Plan shall consist of control

policies and procedures in accordance with standard industry practices for project administration, execution and tracking.

The Program Management Plan shall include the following:

a. Identification of milestones where Government information, activity, equipment, material, facilities, etc. is required and timeline dependencies or prerequisites for subsequent Contractor activities;

b. An Integrated Master Management Plan (IMMP) describing the Contractor's overall management approaches, policies and procedures including suggested project metrics; and,

c. A detailed staffing plan with key personnel approved by the Government.

e. The Contractor shall provide a detailed measurement specification **(Deliverable 19)** for each measurement. This specification shall include, but not be limited to, indicators, derived measures, and base measures. The Contractor shall also provide a Measurement Specification form. Refer to "Acquisition Measurement" a Collaborative Project for PSM for sample measures ttps://www.psmsc.com.

- A completed Acceptance Criteria Plan **(Deliverable 17)** that will identify criteria for acceptance of each deliverable, routing, general contents and related information that will assure that each deliverable is consistent, timely and contains the required information to be used by both the Contractor and the Government to assure the quality of each deliverable.

The Contractor shall develop and maintain a risk register **(Deliverable 4)** and issues register **(Deliverable 26)** containing the following fields:

- Opening date
- Title
- Short description
- Probability Ranking
- Impact Ranking
- An assigned person responsible for its resolution
- Date by which the risk/issue must be resolved
- Mitigation/Response Plan

Current Status

2.1.2.3 Monthly Progress Report (MPR)

The Contractor shall prepare and deliver a Monthly Progress Report **(Deliverable 5)**, format to be provided by the Government. The MPR shall outline deliverables submitted; problems encountered; and schedule deviations. The MPR shall measure the Contractor's price and schedule performance using a mutually agreed upon by the Government and the Contractor. The report shall include the current price and level of effort (i.e., hours worked by task). The Contractor shall identify and communicate to the Government lessons learned along with changes planned in response to lessons learned during the remaining execution of this order.

2.1.2.4 Kick Off & Program Reviews

The Contractor shall schedule and conduct a kick-off meeting in coordination with the Government. The Contractor shall meet with the Government to present an overview of their approach and establish schedules, procedures, and points of contact necessary to conduct the tasks outlined herein. The primary outcome of this meeting is to come to an agreement on the cost, schedule, and performance baselines.

2.1.2.5 Quality Assurance

2.1.2.5.1 Quality Control Plan

The Contractor shall prepare and adhere to a Quality Control Plan (Deliverable 11), developed according to industry standards such as IEEE. Contractor will be compliant to IEEE Std.1028™-2008 Inspection process or equivalent. The draft QCP will initially be submitted five (5) business days after task order start date. Once approved, the QCP becomes final and unless modified, governs all QA procedures for the balance of the contract performance. The final QCP shall be submitted within thirty (30) calendar days following award.

The QCP shall document the Contractor's process that will meet and comply with the quality standards established in this SOW. At a minimum, the QCP must include a self-inspection plan, an internal staffing plan, and an outline of the procedures that the Contractor will use to maintain quality, timeliness, responsiveness, customer satisfaction, and any other requirements set forth in this solicitation.
Additionally, the QCP will document the Contractor's process for:
Establishment and documentation of capable processes,
Internal monitoring and control of critical processes to minimize product variation,
Establishment of mechanisms for feedback of field performance,
Implementation of an effective root cause analysis and corrective action system, and
Continuous process improvement.

During performance of the contract, the Contractor shall maintain a QA inspection system that contains procedures and processes that are consistent with the monitoring and control processes identified in the approved QCP.

The Contractor shall maintain records documenting all corrective actions and process improvements undertaken during contract performance. The records shall validate the Contractor's compliance with the processes contained in the QCP. The Contractor shall make the records available to the Government during contract performance.

The Government has the right to perform periodic surveillance of the Contractor to assure that the Contractor's work products and QA processes are in compliance with the contract requirements, including performing Root Cause Analysis (RCA) on specific problems and/or issues. The Government and the Contractor will coordinate Government surveillance in a manner that will not unduly delay or disrupt the Contractor's performance of the contract

2.1.2.6 Program Reviews – Deliverables 8, 8a, and 8b

The Contractor shall prepare for, conduct or participate in, and report on, both formal and informal reviews and inspections with the Government to review progress and status of activities under this task order. Each review shall provide insight into expenditures, staffing, progress, risks, and status of Government Furnished Equipment (GFE). The Contractor shall provide project briefings addressing cost/price, schedule, performance, and status of each key element of this task order, noting any problems or risks and alternative and recommended solutions. Although the Government may provide meeting space and limited support, including time and date coordination for the IPR, it is the Contractor's responsibility to prepare for, conduct the meeting and provide necessary follow up.

The Contractor shall ensure that all appropriate materials (**Deliverables 8 and 8a**) are provided to Government participants five (5) business days prior to the meeting and that data presented at program reviews is current within not more than five (5) business days. These materials shall include an agenda, a status report, an updated risk register, an updated resource-and-cost-loaded schedule, and an updated action items list.

The Contractor shall prepare and submit a **Weekly Activity Report (Deliverable 8)** to supply information that the Task Manager and other designated individuals might need to make decisions regarding the efforts under this delivery order. For each project task area of the CWBS the report shall contain a synopsis of the tasking, status of tasks, outstanding issues and expected resolution dates and key risks/issues. Items to be tracked in this report will include, at a minimum, open technical questions, risk and issues register, requests for information, and requests for documentation.

The Contractor shall develop and maintain an **Action Items List** (**Deliverable 8a)** to document and monitor tasks, activities, or actions identified for resolution. The action items list shall contain, at a minimum, the following fields:

- Action item number and associated CWBS number
- Date when the action item is identified or created
- Name of the person to whom the action is assigned
- Title and description of the action
- Resolution

Following each meeting, the Contractor shall prepare and provide **Meeting Minutes (Deliverable 8b)** to each Government attendee within two (2) business days following the meeting.

In compliance with current DoD direction, the Contractor shall coordinate actively and responsively with the Government and other Government designated Contractors participating in the design, development, test, implementation, deployment, and operation of the CHCS, AHLTA, and related MHS products. Failure or refusal to coordinate and cooperate with DHCS Integrated Product Teams (IPTs) or IPT member Contractors precludes effective performance of this task order.

2.1.2.7 Quarterly Performance Management Review – Deliverable 9

The Contractor must participate in a quarterly task order performance review meeting with the DHCS leadership. The Contractor must prepare and submit a Quarterly Performance Management Review Report to support an objective examination of contractual performance **(Deliverable 9)**.

2.1.2.8 Weekly Activity Report – Deliverable 8

The Contractor must prepare and submit a Weekly Activity Report that summarizes key activities, key risks, and financial expenditures by WBS element for the preceding week **(Deliverable8)**.

2.1.2.9 Contingency Operations Plan – Deliverable 24 and Deliverable 25

The Contractor shall develop and submit a Contingency Operations Plan to the Government to specify planning for the remediation of specific systems, equipment, software, and/or operations in the event of critical impact resulting from natural, accidental or intentional events. The Contingency Operations Plan shall be due ten (10) calendar days after the award of the order, and will be updated on a quarterly basis **(Deliverable 24)**. The Contingency Operations Plan shall document Contractor plans and procedures to maintain DHA support during an emergency. The Contingency Operations Plan shall include the following:

- A description of the Contractor's emergency management procedures and policy

- A description of how the Contractor will account for their employees during an emergency
- Planned temporary work locations or alternate facilities
- How the Contractor will communicate with DHA during emergencies
- A list of primary and alternate Contractor points of contact, each with primary and alternate:
    - Telephone numbers
    - E-mail addresses
- Procedures for protecting Government furnished equipment (if any)
- Procedures for safeguarding sensitive and/or classified Government information (if applicable)
- Artifacts that the contractor has done simulation tests using this plan (minutes from the simulation which include date and time), lessons learned, identified areas of improvement and changes made to satisfy, etc.
- Plan for types of emergencies, schedule of how often the plan will be updated and tested and to which type of emergency it is tested against.

The Contractor shall provide the COOP plan and disaster recovery strategy **(Deliverable 24)** for the product. The Business Continuity Plan (BCP) **(Deliverable 25)** for the product shall also be provided. The COOP plan shall account for (Recovery Time Objective) RTO and Recovery Point Objective (RPO) identified by the COR. The COOP plan shall be produced in collaboration with the integration vendor and the DHCS operations team. The COOP plan shall adhere to standards set by DHCS.

2.1.2.10 Operations During Emergency Situations

Individual contingency operation plans shall be activated immediately after determining that an emergency has occurred, shall be operational within twelve (12) hours of activation, and shall be sustainable until the emergency situation is resolved and normal conditions are restored or the contract is terminated, whichever comes first. In case of a life threatening emergency, the COR shall immediately make contact with his Contractor Task Managers to ascertain the status of any Contractor personnel who were located in Government controlled space affected by the emergency. When any disruption of normal, daily operations occur, Contractor Task Managers and Contracting Officer Representatives (CORs) shall promptly open an effective means of communication and verify:

- Key points of contact (Government and Contractor)
- Temporary work locations (alternate office spaces, telework, virtual offices, etc.)
- Means of communication available under the circumstances (i.e., email, webmail, telephone, FAX, courier)
- Essential work products expected to continue production by priority

The Government and Contractor Task Managers must make use of the resources and tools available to continue DHA contracted functions to the maximum extent possible under emergency circumstances. Contractors must obtain approval from the COR and Contracting Officer prior to incurring costs over and above those allowed for under the terms of this task order. Regardless of contract type, and of work location, Contractors performing work in support of authorized tasks within the scope of their contract shall charge those hours accurately in accordance with the terms of this task order.

2.1.2.11 Contractor Personnel Performance/Replacement

Substitutions of proposed Key Personnel shall not be allowed for a period of six months after award, except under extreme circumstances. Any substitution or replacement Key Personnel shall have qualifications equal to or greater than the individuals replaced. For temporary and/or permanent replacement of Key Personnel, the Contractor shall provide a resume for each individual to the COR. Resumes shall be provided at least two weeks (or as mutually agreed upon) prior to making any personnel changes. The Government reserves the right to pre-approve any replacement or substitution of Key

Personnel. Contractor personnel shall submit necessary information to be issued a clearance prior to reporting for performance.

2.1.2.12 Transition Support

2.1.1.12.1 Transition In Support

The Contractor shall provide a Transition-In Plan not later than (NLT) 5 business days following the Kick-off Meeting. This plan shall provide for sixty (60) calendar days incoming transition for transitioning work from an active task order to this follow-on task order.

The contractor shall perform the following activities during the transition-in period:

- **Participate in a Task Order Kick-off Meeting as scheduled following award**
- **Provide a transition-in plan of action and milestone (POA&M) schedule to the Government. (Deliverable 15a)**
- **Establish procedures with the outgoing contractor to ensure transition of operations, maintenance, and logistics functions without any degradation of service**
- **Perform joint inventories and inspections of all government furnished property with the government and outgoing contractor relevant to the performance of the contract**
- **Establish procedures with the outgoing contractor to transition operations, maintenance, and logistics functions while maintaining service. This includes defining processes for turn-over of system administration, accounts, privileges, and accesses**
- **Provide weekly updates to the Government to track progress of the transition-in plan schedule and provide any issues or concerns.**

2.1.2.12.2 Transition Out Support

In accordance with this task order, and due to the importance of having a comprehensive plan *prior* to opting for this task the Contractor shall provide a detailed Outgoing Transition Plan **(Deliverable 15b)** that includes a comprehensive listing of activities such as those listed below, that demonstrates their understanding of all the tasks involved with a transition-out as well as a timeline on when those tasks would best be conducted for the benefit of the Government. This plan shall provide for sixty (60) calendar days outgoing transition for transitioning work from an active task order to a follow-on contract/order or Government entity. This transition may be to a Government entity, another Contractor or to the incumbent Contractor under a new contract/order. In accordance with the Government-approved plan, the Contractor shall assist the Government in planning and implementing a complete transition from this Contract and/or orders issued under this Contract to a successful provider. This shall include formal coordination with Government staff and successor staff and management. It shall also include delivery of copies of existing policies and procedures, and delivery of required metrics and statistics. This transition plan shall be in accordance with the DHCS Transition Plan guidance that includes:

- Coordination with Government representatives,
- Review, evaluation and transition of current support services,
- Transition of historic data to new Contractor system,
- Government-approved training and certification process,
- Transfer of hardware warranties and software licenses,
- Transfer of all System/Tool documentation to include, at a minimum: user manuals, system administration manuals, training materials, disaster recovery manual, requirements traceability matrix, configuration management documents and all other documents required to operate, maintain and administer systems and tools,
- If another Contractor follows this Contractor with work related to this work, this Contractor will provide any developed source code (compiled and uncompiled, including all versions, maintenance updates and patches) with written instructions for the source code on which this

Contractor has worked, so that an experienced software engineer, previously not familiar with the source code can understand and efficiently work with the source code. In addition, this Contractor will provide for 90 calendar days, a software engineer (or person of comparable work level) with significant experience working with the source code, to assist the new Contractor,

- Orientation phase and program to introduce Government personnel, programs, and users to the Contractor's team, tools, methodologies, and business processes,
- Disposition of Contractor purchased Government owned assets, including facilities, equipment, furniture, phone lines, computer equipment, etc.,
- Disposition of tool(s) and/or emulator(s) used to test the developed product,
- Transfer of Government Furnished Equipment (GFE) and Government Furnished Information (GFI), and GFE inventory management assistance,
- Applicable DHA debriefing and personnel out-processing procedures,
- Turn-in of all government keys, ID/access cards, and security codes.

2.1.2.14 Closeout Briefing

The Contractor shall provide a briefing to the Government **(Deliverable 22)** at least 10 business days prior to the end of the Period of Performance including:

- A list of all contract deliverables and their delivery dates
- A final presentation of schedule and cost throughout the project lifecycle
- A final Lessons Learned Report

3.0 Deliverables

All deliverables shall be submitted to the DHA and GSA CORs, and to the Fiscal, Project, and Technical Support contacts who shall be identified by the COR. The Contractor shall also submit all deliverables to the Contract Deliverables Requirements List (CDRL) Support Center and the Configuration Management (CM) Library Support Center at the following addresses:

Organization:	DHCS
ATTN:	CDRL Support Center
POC:	Mark Svenson
Address:	5109 Leesburg Pike, Suite 508
	Falls Church, VA 22041-3206
Phone Number:	(703) 882-3948
Email Address:	DHCS.CM.CDRL@dha.mil

Organization:	DHCS
ATTN:	CM Library Support Center
POC:	Kelley Chang
Address:	5109 Leesburg Pike, Suite 817
	Falls Church, VA 22041-3206
Phone Number:	(703) 882-3936
Email Address:	Kelley.M.Chang.ctr@mail.mil
Cc:	ThuyDung.T.Truong.ctr@mail.mil

3.1 Method of Delivery

CDRL Support Center Method of Delivery

Electronic copies (in Microsoft Office document format) shall be delivered by the Contractor to the CDRL Support Center directly into the automated tool in use (currently SBM – Serena Business

Mashups). Physical delivery will be allowed on an exception basis only with the individual case approval of the COR. Physical delivery, when authorized, shall be via FedEx or UPS.

CM Library Support Center Method of Delivery
The Contractor shall deliver electronic copies to the CM Library via the SVM (Serena Version Manager), or by physical delivery as approved by the COR. Physical delivery, when authorized, shall be via FedEx or UPS.

3.2 Government Acceptance Period

The Government will have twenty (20) business days to review draft deliverables and make comments. The Contractor shall have five (5) business days to make corrections. Upon receipt of the final deliverables, the Government will have five (5) business days for final review prior to acceptance or providing documented reasons for non-acceptance. When the Government fails to complete the review within the review period, the deliverable will become acceptable by default.

The Government will have the right to reject or require correction of any deficiencies found in the deliverables. In the event of a rejected deliverable, the Contractor will be notified in writing by the Government of the specific reasons for rejection. The Contractor shall have five (5) business days to correct the rejected deliverable and return it per delivery instructions.

3.3 Delivery Schedule Abbreviations

The following abbreviations are used in the delivery / deliverable schedule:

Abbreviation	Definition
AM	Acquisition Manager
CDRL	CDRL Support Center
CM	CM Library
COR	Contracting Officer's Representative for the Task Order
DA	Days after
DACA	Days after contract award (award of this order)
DAEOM	Days after end of month
Days	Calendar Days unless otherwise specified
E	Electronic Copy
H	Hard Copy
KO	Contracting Officer
NLT	Not Later Than
WDA	Working Days After

3.4 Deliverable / Delivery Schedule

A summary of deliverables follows.

Standard Item	TS Ref	Title	Dist	Initial	Subsequent
Deliverable 1	6.1	Non-Disclosure Agreement	COR CDRL	Signed statements are due, from each employee assigned, prior to performing ANY work on this task.	
Deliverable		Subcontract	COR	N/A	N/A

3		Management Plan	CDRL CM		
Deliverable 4	2.1.2.2 2.1.2.8	Risk Register	COR CDRL CM	Draft due five (5) business days after kick-off meeting	Weekly, NLT the 2nd business day
Deliverable 5	2.1.2.3	Monthly Progress Report (MPR)	COR CDRL CM	Monthly, NLT 45 calendar days after task order start date	Monthly, NLT 15 DAEOM
Deliverable 7	2.1.2.1	Program management Plan (PMP)	COR CDRL CM	Draft due five (5) business days after task order start date	30 business days after task order start date
Deliverable 8	2.1.2.6 2.1.2.8	Weekly Activity Report	COR CDRL CM	5 business days before each weekly progress review meeting	NLT the last business day of each week
Deliverable 8a	2.1.2.6	Program Review Action Items List	COR CDRL CM	5 business days after the kick-off meeting and then 5 business days prior to each weekly progress review meeting	Weekly
Deliverable 8b	2.1.2.6	Program Review Meeting Minutes	COR CDRL CM	2 business days after each weekly progress review meeting	Weekly
Deliverable 9	2.1.2.7	Quarterly Performance Management Review	COR CDRL CM	Quarterly	NLT the last business day of each quarter
Deliverable 11	2.1.2.5.1	Quality Control Plan	COR CDRL CM	Draft due five (5) business days after task order start date	30 business days after task order start date
Deliverable 14	NA	NA	NA	NA	NA
Deliverable 15a	2.1.2.12.1	Transition In Plan	COR CDRL CM	5 business days after kick off meeting	NA
Deliverable 15b	2.1.2.12.2	Outgoing Transition Plan	COR CDRL CM	NLT 120 calendar days before end of the period of performance	NLT 90 calendar days before end of the period of performance
		NA		raf NA	NA
Deliverable 17	2.1.2.2	Acceptance Criteria Plan (ACP)	COR	Draft due five (5) business days after task order start date	5business days after task order start date; Update if required
Deliverable 19	2.1.2.2	Measurement Specifications	COR CDRL CM	30 business days after task order start date	Monthly
Deliverable	5. 6	Security	COR	Draft due five (5) business days	10 business

20		Management Plan	CDRL CM	after task order start date	days after the SSR
Deliverable 21	NA	NA	NA	NA	NA
Deliverable 22	2.1.2.14	Closeout Briefing	COR CDRL CM	10 business days prior to the end of the Period of Performance	Annually
		NA		NA	NA
Deliverable 24	2.1.2.9	COOP plan and Disaster Recovery Manual	COR CDRL CM	10 business days after task order start date	Review quarterly and update if required
Deliverable 25	2.1.2.9	Business Continuity Plan	COR CDRL CM	10 business days after task order stat date	Review quarterly and update if required
Deliverable 26	2.1.2.2	Issues Register	COR CDRL CM	Draft due five (5) business days after task order start date	Monthly, NLT 15 DAEOM
Deliverable 27	1.3.1	Tier III Triage Policy	COR CDRL CM	30 business days after task order stat date	Review monthly and update if required
Deliverable 28	1.3.2	Tier II.5 Trouble Ticket Resolution Process	COR CDRL CM	30 business days after task order start date	Review monthly and update if required
Deliverable 29	1.3.12.1	Theater Data Reconciliation Users Guide	COR CDRL CM	30 business days after task order start date	Review monthly and update if required
Deliverable 30	1.3.12.2	Updated Theater Data Reconciliation Users Activities	COR CDRL CM	45 business days after task order start date	Weekly, NLT the 2nd business day. (First Option period, if exercised, deliverable follows the same submission requirement.)
Deliverable 31	1.3.7	Decision Matrix	COR CDRL CM	45 business days after task order start date	Monthly
Deliverable 32	1.3.7	Risk Register	COR CDRL CM	45 business days after task order start date	Monthly

4.0 Contract Administration

4.1 Place of Performance
The Contractor shall perform at the Contractor's facility.

4.2 Period of Performance
The period of performance for this contract shall be one base year of twelve months and four twelve month option periods, to begin on April 10, 2016 or date of award, whichever is later, as follows:

Base Year -	April 10, 2016 to April 09, 2017
Option Year 1 -	April 10, 2017 to April 09, 2018
Option Year 2 -	April 10, 2018 to April 09, 2019
Option Year 3 -	April 10, 2019 to April 09, 2020
Option Year 4 -	April 10, 2020 to April 09, 2021

The Government shall have the unilateral right to exercise option periods in accordance with FAR Clause 52.217-9 Option to Extend the Term of the Contract:
a) The Government may extend the term of this contract by written notice to the Contractor within thirty (30) calendar days of the contract expiration date; provided that the Government shall give the Contractor a preliminary written notice of its intent to extend at least sixty (60) calendar days before the contract expires; alternately the absence of written notice does not preclude the Government from exercising the option periods. The preliminary notice does not commit the Government to an extension.
b) If the Government exercises this option, the extended contract shall be considered to include this option clause.

The total duration of this contract, including the exercise of any options under this clause, shall not exceed sixty (60) months; with the exception of any potential bridge of the contract for an emergency continuance of contract performance to be awarded for the benefit of the Government.

4.3 Recognized Holidays: The Contractor shall not perform on the following Government holidays:

New Year's Day	Labor Day
Martin Luther King Jr.'s Birthday	Columbus Day
President's Day	Veteran's Day
Memorial Day	Thanksgiving Day
Independence Day	Christmas Day

4.4 Points of Contact

Government Customer Representative:
TBD
300 Convent Street, Suite 1800
San Antonio, TX 78205

GSA ITM/COR:
Christopher Lauer
Region 3 FAS
4200 Miars Quay
Chesapeake, VA 23321
Voice: 757-483-5815
Fax: 757-483-5821

Email: christopher.lauer@gsa.gov

GSA Contracting Specialist:
Susan Cameron
Region 3 FAS
The DOW Building
100 S Independence Mall W
Philadelphia, PA 19106
Phone: 215-446-5859
Fax: 215-814-6160
Email: susan.cameron@gsa.gov

GSA Contracting Officer
Katrina Lloyd
Region 3 FAS
The DOW Building
100 S Independence Mall W
Philadelphia, PA 19106
Phone: 215-446-4898
Fax: 215-829-2826
Email: katrina.lloyd@gsa.gov

4.5 Quality Assurance Surveillance Plan (QASP)

In accordance with the Quality Assurance Plan, to be provided as a separate attachment, the Government will document overall satisfaction with contractor performance through review and evaluation of the contractor's success in meeting the standards and measures outlined in the following performance metrics table:

Task	Indicator	Standard	Acceptable Quality Level	Method of Surveillance	Incentive
1. Paragraph 1.3.1 - Triage Trouble Tickets	Tickets elevated for Tier III action will be validated by the contractor per the contractor developed triage policy	100% of Tier III trouble tickets will be validated by the contractor within 12 hours of receipt	98% of tickets elevated requesting Tier III support will be correctly elevated for Tier III support	Monthly review of Tier II logs for incorrectly classified Tier III requests check of submission logs	Exercise of Option Period and past performance
2. Paragraph 1.3.6.1 - Trouble Ticket Tracking	Availability of trouble ticket status to DHIMS leadership	All trouble tickets submitted from the customer will be categorized, validated, tracked, and available for DHIMS leadership review no later than 24 hours of initiation by customer	98% of all trouble tickets logged will be available for DHIMS leadership review no later than 24 hours of initiation by the customer	Review of trouble ticket logs by DHIMS leadership	Exercise of Option Period and past performance

Task	Indicator	Standard	Acceptable Quality Level	Method of Surveillance	Incentive
3. Paragraph 1.3.7 - Monthly Performance Reporting	Metrics identified in paragraph 1.3.7 will be submitted to DHIMS leadership NLT the 10th day of the month for performance through the end of the previous month	All proposed metrics will be tracked, analyzed, and submitted in final report format NLT the 10th day of the month following the previous month	Reports will be submitted NLT the 15th of the month	Review of reports by DHIMS leadership	Exercise of Option Period and past performance

4.6 Government Furnished Equipment (GFE)/ Information (GFI)/Property

The Contractor shall maintain a detailed inventory accounting system for Government Furnished Equipment/Material. The inventory accounting system must specify, as a minimum: product description (make, model), Government tag number, date of receipt, name of recipient, location of receipt, current location, and contract/order number under which the equipment is being used. The Contractor shall either: a) attach an update inventory report to each Monthly Progress Report, or b) certify that the inventory has been updated and is available for Government review. In either case the Contractor's inventory listing must be available for Government review within one business day of COR request.

For any GFI provided the Contractor shall comply with all DHA security requirements.

4.7 Section 508

The Contractor shall support the Government in its compliance with Section 508 throughout the development and implementation of the work to be performed. Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. 794d) requires that when Federal agencies develop, procure, maintain, or use electronic information technology, Federal employees with disabilities have access to and use of information and data that is comparable to the access and use by Federal employees who do not have disabilities, unless an undue burden would be imposed on the agency. Section 508 also requires that individuals with disabilities, who are members of the public seeking information or services from a Federal agency, have access to and use of information and data that is comparable to that provided to the public who are not individuals with disabilities, unless an undue burden would be imposed on the agency. Applicable standards are 1194.21-1194-26. Additional Section 508 information can be found at the following websites: https://www.section508.gov

4.8 Personal Services

The client has determined that use of the GSA requirements contract to satisfy this requirement is in the best interest of the Government, economic and other factors considered, and this task order is not being used to procure personal services prohibited by the Federal Acquisition Regulation (FAR) Part 37.104 titled "Personal Services Contracts".

4.9 Travel and Other Direct Costs

Travel and Other Direct Costs are not required for this task order.

4.10 Invoicing

The Period of Performance (POP) for each invoice *shall* be for one calendar month. The contractor *shall* submit only one invoice per month per order/contract. The appropriate GSA office will receive the invoice by the twenty-fifth calendar day of the month after either:

(1) The end of the invoiced month (for services) or

(2) The end of the month in which the products (commodities) or deliverables (fixed-priced services) were delivered and accepted by the Government.

For Firm-Fixed Price orders/contracts: FFP CLINs shall be charged as 1/nth of the overall price of the n-month performance period. For example, with a 12-month performance period, monthly invoices shall reflect 1/12th of the overall value of the FFP CLIN for the 12-month period.

For Labor Hour and Time and Material orders/contracts each invoice *shall* show, the skill level category, the hours worked per skill level, the rate per skill level and the extended amount for that invoice period. It *shall* also show the total cumulative hours worked (inclusive of the current invoice period) per skill level, the hourly rate per skill level, the total cost per skill level, the total travel costs incurred and invoiced, and the total of any other costs incurred and invoiced, *as well as* the grand total of all costs incurred and invoiced.

For Labor Hour and Time and Material orders/contracts each invoice *shall clearly indicate* both the current invoice's monthly "burn rate" and the total average monthly "burn rate".

The contractor *shall submit* all required documentation (unless exempted by the contract or order) as follows:

For Travel: Submit the traveler's name, dates of travel, location of travel, and dollar amount of travel.

For ODCs: Submit a description of the ODC, quantity, unit price and total price of each ODC.

Note: The Government reserves the right to audit, thus; the contractor shall keep on file all backup support documentation for travel and ODCs.

Note: For Firm Fixed Price, Labor Hour, and Time and Material fiscal task items:

Charges:

- All invoice charges must be task item specific (only one task item) unless concurrent task item periods of performance exist.

- For invoices with concurrent task item periods of performance all invoice charges must be service month specific (that is one service month only).

Credits:

- If the credit invoice is for the same year of a particular ACT#, the contractor shall include that credit on a subsequent invoice submission against that same ACT#. If the contractor is unwilling to offset a subsequent invoice then they must submit a refund check.

- When the credit invoice is for a different year, the contractor shall submit a refund check for that credit invoice.

Invoices that net to a credit balance **SHALL NOT** be accepted. Instead a refund check must be submitted by the contractor to GSA accordingly. The refund check shall cite the ACT Number and the period to which the credit pertains. The contractor shall provide the credit invoice as backup documentation. Do not attach credit invoice in ITSS or on the Finance website. It must be attached to the refund check. The refund check shall be mailed to:

General Services Administration
Finance Division
P.O. Box 71365
Philadelphia, PA 19176-1365

Posting Acceptance Documents: Invoices shall be submitted monthly through GSA's electronic Web-Based Order Processing System, currently ITSS to allow the client and GSA COTR to electronically accept and certify services received by the customer representative (CR). Included with the invoice will be all back-up documentation required such as, but not limited to, travel authorizations and training authorizations (including invoices for such).

Receiving Agency's Acceptance: The receiving agency has the following option in accepting and certifying services;

a. Electronically: The client agency may accept and certify services electronically via GSA's electronic Web-Based Order Processing System, currently ITSS, by accepting the Acceptance Document generated by the contractor. Electronic acceptance of the invoice by the CR is considered concurrence and acceptance of services.

Electronic acceptance of the invoice by the CR is considered concurrence and acceptance of services. The contractor shall seek acceptance and electronically post the acceptance document in GSA's electronic Web-based Order Processing System, currently ITSS. After acceptance of the invoice by the CR, the Contractor shall submit a proper invoice to GSA Finance (*www.finance.gsa.gov/defaultexternal.asp*) not later than five (5) business days after acceptance by the Government of the product, service, and/or cost item.

Note: The acceptance of the authorized agency customer representative is REQUIRED prior to the approval of payment for any invoiced submitted and shall be obtained prior to the approval of payment. In order to expedite payment, it is *strongly recommended* that the contractor continue to include the receiving agency's electronic acceptance of all the services or products delivered, with signature of the authorized agency customer representative and the date of acceptance, as part of the submission documentation.

Note: If *any* invoice is received without the required documentation and the customer's electronic acceptance, the invoice *shall* be rejected in whole or in part as determined by the Government.

Posting Invoice Documents: Contractors shall submit invoices to GSA Finance for payment, after acceptance has been processed in GSA's electronic Web-Based Order Processing System, currently ITSS. The contractor is to post the invoice on GSA's Ft. Worth web site, *www.finance.gsa.gov/defaultexternal.asp*

Content of Invoice: The contractor's invoice will be submitted monthly for work performed the prior month. The contractor may invoice only for the hours, travel and unique services ordered by GSA and

actually used in direct support of the client representative's project. The invoice shall be submitted on official letterhead and shall include the following information at a minimum.

1. GSA Task Order Number
2. Task Order ACT Number
3. Remittance Address
4. Period of Performance for Billing Period
5. Point of Contact and Phone Number
6. Invoice Amount
7. Skill Level Name and Associated Skill Level Number
8. Actual Hours Worked During the Billing Period
9. Travel Itemized by Individual and Trip (if applicable)
10. Training Itemized by Individual and Purpose (if applicable)
11. Support Items Itemized by Specific Item and Amount (if applicable)

Final Invoice: Invoices for final payment must be so identified and submitted within 60 calendar days from task completion and no further charges are to be billed. A copy of the written acceptance of task completion must be attached to final invoices. The contractor shall request from GSA an extension for final invoices that may exceed the 60-business day time frame.

The Government reserves the right to require certification by a GSA COTR before payment is processed, *if necessary*.

Close-out Procedures.

General: The contractor shall submit a final invoice within sixty (60) calendar days after the end of the Performance Period. After the final invoice has been paid the contractor shall furnish a completed and signed Release of Claims (GSA Form 1142) to the Contracting Officer. This release of claims is due within fifteen (15) calendar days of final payment.

5.0 Program/System Security

The Contractor shall establish appropriate administrative, technical, and physical safeguards to protect any and all Government data, to ensure the confidentiality, integrity, and availability of Government data. As a minimum, this shall include provisions for Program/System Security, Risk Management Framework Support, Information Assurance Vulnerability management (IAVM), Public Key Infrastructure, Physical Security, Personnel Security, Security Design and Configuration, Identification and Authentication, Enclave and Computing Environment, Physical and Environmental, Continuity, Vulnerability and Incident as listed.

The Contractor shall ensure that Cybersecurity (CS) is fully integrated into all phases of the software development process, including initial design, development, testing, and is part of the Preliminary Design Review, Critical Design Review, and Test Readiness Review approval process. The Contractor shall plan for the Risk Management Framework (RMF) for DoD Information Technology (IT), as defined in DoDI 8510.01, in parallel with the Software Development Lifecycle to ensure that prior to implementation; the system is assessed and authorized. Based on the assigned categories for Confidentiality, Availability, and Integrity, IA controls applicable to software shall be identified as requirements and implemented in accordance with DoD Instruction 8500.1 "Cybersecurity" March 14, 2014. The Contractor shall ensure that appropriate Defense Information Systems Agency Security Technical Implementation Guides

(STIGs), National Institute of Standards and Technology (NIST) standards and National Security Agency Security Configuration Guides pertaining to software are implemented. The Contractor shall implement Information Assurance Vulnerability Management and US Cyber Command issuances and orders pertaining to software throughout the development, deployment, and operational processes. The Contractor shall deliver to the Government software that is compliant with the requirements of the DOD cybersecurity program. The Contractor shall ensure all system supporting Operating Systems (OS), Database Management Systems (DBMS) Web Applications remote monitoring, application development, etc. conform to the requirements outlined in all applicable Defense Information Security Agency (DISA) Security Technical Implementation Guides (STIG), NIST, and SRG's.

5.1 Risk Management Framework (RMF) for DOD Information Technology (IT) Support

Authorization by the DHA Authorizing Official is the formal approval by the Government to operate IS/networks in a particular security mode using a prescribed set of safeguards at an acceptable level of risk. In addition, authorization allows IS/networks to operate within the given operational environment with stated interconnections; and with appropriate level of protection for the specified period.

The Contractor shall provide required support to ensure the continuation of DHCS-owned, Contractor-managed system/network Authorization in compliance with DHA Cybersecurity, DHCS, TMIP, DISA, DOD, and Military Service requirements. In accordance with the DOD Risk Management Framework (RMF) for DoD Information Technology (IT), the Contractor shall provide the artifacts required to validate compliance with DoDI 8500.1 CS and NIST SP 800-53 controls necessary to support the evaluation of a DHCS systems based on the assigned categories associated with the system/application for confidentiality, availability, and integrity. The Contractor shall make available all persons and products necessary to support the validation of the security of the developed product(s) and supporting sites.

The Contractor shall develop and maintain the system security documentation necessary to support the Risk Management Framework (RMF) for DoD Information Technology (IT) as outlined in DoD Instruction 8510.01. The Contractor shall identify all changes affecting the architecture of systems or sites for which it is responsible for the development, operations, and maintenance. The Contractor shall provide updated documentation outlining the proposed architecture changes to the contracting officer for review by the DHCS ISSM prior to making such changes. Proposed architectural changes shall be presented to the DHCS ISSM nine months prior to expected deployment. Once approved, the Contractor shall update all applicable RMF documentation to include the approved design. At this time the Contractor shall provide the support necessary to ensure the successful assessment update or full Assessment and Authorization (A&A) activities to include:

- Assessment Kick-off
- Documentation updates
- Security assessment support
- Remediation activities
- Mitigation validation support
- Reciprocity support

The Contractor shall comply with RMF requirements, as specified by the Government that meet appropriate DOD Cybersecurity requirements. The RMF requirements shall be met before the Contractor's system is authorized to access DOD data or interconnect with any DOD IS/network that receives, processes, stores, displays or transmits DOD data. The Contractor shall initiate the RMF process by providing the Contracting Officer, within 60 calendar days following task order start date, the required documentation necessary to receive an Approval to Operate (ATO). The Contractor shall make its IS/networks available for testing, and initiate the RMF testing four months (120 calendar days) in

advance of accessing DoD data or interconnecting with DoD IS/networks. The Contractor shall ensure the proper Contractor support staff is available to participate in all phases of the RMF process. This includes, but is not limited to:

- Attending and supporting RMF meetings with the Government
- Supporting/conducting the vulnerability mitigation process
- Supporting the Assessment Team during system security testing
- Contractors must confirm that their IS/networks are locked down prior to initiating testing.
- Confirmation of system lock down shall be agreed upon during the definition of the A&A boundary and be signed and documented as part of the System Security Authorization Agreement (SSAA)
- Locking down the system means that there shall be no changes made to the configuration of the system (within the A&A boundary) during the S&A process

Any re-configuration or change in the system during the A&A testing process will require a re-baselining of the system and documentation of system changes.

Vulnerabilities that have been identified by the Government as "must-fix" issues during RMF process must be mitigated according to the timeline identified by the Government Representative. RMF checklists are provided for complying RMF requirements.
A request for a waiver to RMF requirements may be submitted for temporary testing and other usual circumstances. A waiver request must be submitted, in writing, to the Authorizing Official (AO). The request must include mitigation strategies that ensure adequate protective measures and security controls are in place (for example: air gapping a testing network) to mitigate the risk associated with the waived requirement.

5.2 IAVM
The Contractor shall implement a vulnerability management program. The DOD IAVM program provides protections against known threats and vulnerabilities. The IAVM program requires the registration of DoD IS assets in the DoD Vulnerability Management System (VMS), which allows for the timely dissemination of critical vulnerability information. It also assists in the documentation and tracking of compliance, providing increased cybersecurity to MHS systems and applications. As part of the program, the Contractor shall provide a primary and secondary point of contact in the VMS and to the DHCS Information Assurance Vulnerability Alert (IAVA) Monitor. The point of contact shall provide, upon receipt of a vulnerability message, an acknowledgment of receipt via the VMS. The contactor shall thoroughly test all mitigations for the vulnerability, and upon applying the mitigation to the system, report compliance in the VMS. Receipt and compliance messages to the Government shall occur within the stipulated time window, as stated in the vulnerability message or in the VMS.

The Contractor shall ensure DHA IS assets that are under development are registered in the VMS and have all applicable electronic patches installed for the system (1) when the system is delivered to the Government, or (2) if the DHA IS assets are used to store or process Government data prior to delivery (such as when being used in testing and development). Guidance regarding the requirement for IAVM is contained in the DOD Information Assurance Vulnerability Alert (IAVA) December 30, 1999 memorandum and Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6510.01F, 9 February 2011 provides additional reference information. Implementation is addressed in the Defense Information Systems Agency (DISA) IAVA Process Handbook, Version 2.1, June 11, 2002. An asset is any device on any DoD-owned, controlled or contracted IS or network, to include (but not limited to) workstations, servers, routing devices (routers, switches, firewalls), networked peripherals (e.g., network printers,

portable electronic devices) and controlled interfaces (e.g., guards). A device is considered a node on a network if it has its own network identification (internet protocol (IP) and/or media access control address). The Defense Information System Agency's (DISA) VMS web enabled application is used to disseminate IAVAs Information Assurance Vulnerability Bulletins (IA VBs), and Information Assurance Technical Advisories down to the System Administrator (SA) and applicable personnel throughout the chain of command.

The Contractor shall evaluate the impact of security patches to DHCS-owned, Contractor-managed systems, assets, and networks. The Contractor shall ensure all DHCS-owned, Contractor-managed assets are registered and maintained within the DISA Vulnerability Management System (VMS) in accordance with the MHS IAVM Process. All DHCS system platforms shall be in compliance with all known applicable Vulnerability Notices issued by US Cyber Command. The Contractor shall ensure that all applicable Vulnerability Notices are assessed for applicability. When applicable, the Contractor shall test and document any finding and or configuration changes that need to be made in order to ensure DHCS system hardware and software are not impacted negatively by introduction of the change necessary to mitigate the vulnerability. The Contractor shall update the appropriate VMS registered assets noting the compliance status. Compliance status reporting shall be executed in accordance with the time constraints published within the vulnerability notice.

The Contractor shall ensure that all applicable vulnerability fixes/patches are available to be issued to the field within a scheduled build or, when necessary, as a standalone release package. If a vulnerability fix or patch is determined to be applicable, the Contractor shall provide notification to the applicable system's Product team so that it can be coordinated and tracked in accordance with the DHCS Configuration Management and Release Management process. The Contractor shall ensure that the release packages addressing vulnerability notices include test results, installation instructions, configuration changes, and any other information needed to ensure the successful implementation of the vulnerability notice. The Contractor shall submit the release package to DHCS CM in accordance with CM Intake and Distribution guidance.

5.3 Public Key Infrastructure

The Contractor shall follow DODI 8520.02, Public Key Infrastructure (PKI) and Public Key (PK) Enabling dtd, May 24, 2011, DODI 8520.03, Identity Authentication for Information Systems dtd May 13, 2011 and other relevant DOD standards, policies, and procedures related to the use of Public Key Infrastructure (PKI) certificates and biometrics for positive authentication. Where interoperable PKI is required for the exchange of unclassified and sensitive information between DOD and its Contractors, the Contractor shall obtain all necessary certificates. The Contractor shall turn over to the Government all encryption keys for deployed systems, backdoor algorithms, and procedures for their use in remote support. The Contractor must provide a written report detailing all of the above, prior to task order expiration, regardless of modifications or extensions.

5.4 Physical Security

The Contractor shall employ physical security safeguards for IS/Networks involved in processing or storage of Government Data to prevent the unauthorized access, disclosure, modification, destruction, use, etc., and to otherwise protect the confidentiality and ensure use conforms with DoD regulations. In addition, the Contractor shall support a Physical Security Audit (PSA) of the Contractor's internal information management infrastructure to be performed by the Government. The MHS Physical Security Audit Matrix will be provided by the Government.

The Contractor shall correct any deficiencies identified by the Government of the Contractor's physical security posture. The Contractor shall be required to follow all requirements in the MHS Information Assurance Policy. New MHS policies will be provided by the Government.

5.5 Personnel Security

The Contractor shall comply with DoD Directive 8500.1, "Cybersecurity (CS), DoD Directive 5400.11, "DoD Privacy Program", DoD 6025.18-R, "DoD Health Information Privacy Regulation", and DoD 5200.2-R, "Personnel Security Program Requirements."

The Contractor responsibilities for ensuring personnel security include, but are not limited to, meeting the following requirements:

- Follow the DHA Privacy Office guidelines for submittal of Automated Data Processor/Information Technology (ADP/IT) security clearances and ensure all Contractor personnel are designated as ADP/IT-I, ADP/IT-II, or ADP/IT-III where their duties meet the criteria of the position sensitivity designations. Contact the DHA Privacy Office for guidance on the appropriate ADP/IT levels for personnel on the contract. The DHA Privacy Office procedures for personnel security will be provided by the Government Initiate, maintain, and document personnel security investigations appropriate to the individual's responsibilities and required access to Military Health System (MHS) Sensitive Information (SI).
- Immediately report to the DHA Privacy Office and deny access to any automated information system (AIS), network, or MHS SI information if a CONTRACTOR employee filling a sensitive position receives an unfavorable adjudication, if information that would result in an unfavorable adjudication becomes available, or if directed to do so by the appropriate government representative for security reasons.
- Ensure that all Contractor personnel receive information assurance (IA) training before being granted access to DOD AISs/networks, and/or MHS SI information.

The Contractor shall ensure that all Individuals requiring access to sensitive information are processed for access authorization in accordance with DOD personnel security policies. The Contractor shall ensure that all authorized users maintain the appropriate ADP/IT category classification for a position of public trust specific to their role.

The Contractor shall ensure that only individuals who have a valid need-to-know that is demonstrated by assigned official Government duties and who satisfy all personnel security criteria (e.g., IT position sensitivity background investigation requirements outlined in DOD 5200.2-R) are granted access to information with special protection measures or restricted distribution as established by the DHCS.

Specific to DHCS-owned, Contractor-managed systems, The Contractor shall implement a program to ensure that upon arrival and periodically thereafter, all personnel receive training and familiarization to perform their assigned CS responsibilities, to include familiarization with their prescribed roles in all CS related plans such as incident response, configuration management and COOP or disaster recovery.

5.6 Security Design and Configuration

The Contractor shall support comprehensive Cybersecurity (CS) reviews of all DHCS-owned, Contractor-managed information system annually. These reviews will be coordinated with the DCMS Program Office and will be used to evaluate existing CS policies and processes to ensure that they fully support the goal of uninterrupted operations. The Contractor shall produce a Plan of Action and Milestones (POA&M) document identifying the milestones and schedule necessary to remediate any identified vulnerabilities.

The Contractor shall ensure wherever possible all system security designs incorporate the use of single sign-on, PKE, smart cards and biometrics when identification, authentication, and authorization are required.

The Contractor shall ensure that all DHCS-owned Contractor-managed system assets and applications are configured in accordance with the most current Security Technical Implementation Guidance (STIG). The Contractor shall monitor all DHCS-owned Contractor-managed assets for compliance and shall report monthly on the status of each. The Contractor shall provide a detailed report identifying all undocumented control/security configuration violations and shall also provide a high-level report that identifies quantities of category I, II, and III findings to be presented to the COR.

The Contractor shall incorporate all applicable DOD security and Cybersecurity (CS) requirements into the design of any product of this proposal. The Contractor shall present design documentation to DHCS CS representatives prior to product development. Design documentation shall identify the proposed architecture and clearly define the accreditation boundary of the system; the architecture shall specifically:

- Address the Ports, Protocols, and Services (PPS) proposed to be used to transport data and communicate between systems.
- Identify all external interfaces, the information being exchanged, and the protection mechanisms associated with each interface
- Identify user roles required for access control and the access privileges assigned to each role
- Address unique security requirements (e.g., encryption of key data elements at rest)
- Identify categories of sensitive information processed or stored by the AIS application, and their specific protection plans (e.g., Privacy Act, HIPAA)

The Contractor shall ensure that the acquisition or outsourcing of IT services in support of DHCS-owned, Contractor-managed systems addresses Government, service provider, and end user CS roles and responsibilities.

The Contractor shall obtain assurance that the outside entity will appropriately safeguard PHI and that those assurances relate to all exchanges of said PHI, and that any contract/agreement will specify all required element necessary to ensure safeguarding of the data.

The Contractor shall ensure that the use of mobile code in the design of any system or system component meets the following requirements:

- Emerging mobile code technologies that have not undergone a risk assessment by NSA and been assigned to a Risk Category by the DoD CIO is not used.
- Category 1 mobile code is signed with a DoD-approved PKI code signing certificate; use of unsigned Category 1 mobile code is prohibited; use of Category 1 mobile code technologies that cannot block or disable unsigned mobile code (e.g., Windows Scripting Host) is prohibited.
- Category 2 mobile code which executes in a constrained environment without access to system resources (e.g., Windows registry, file system, system parameters, and network connections to other than the originating host) may be used.
- Category 2 mobile code that does not execute in a constrained environment may be used when obtained from a trusted source over an assured channel (e.g., SIPRNET, SSL connection, S/MIME, code is signed with a DoD-approved code signing certificate).
- Category 3 mobile code may be used.

- All DOD workstation and host software are configured, to the extent possible, to prevent the download and execution of mobile code that is prohibited.
- The automatic execution of all mobile code in email is prohibited; email software is configured to prompt the user prior to executing mobile code in attachments.

The Contractor shall incorporate the use of encryption to protect the confidentiality and integrity of sensitive data communications. The Contractor shall ensure that only NIST FIPS 140-2 validated cryptography (e.g., DoD PKI class 3 or 4 token) is used to implement encryption (e.g., AES, 3DES, DES, Skipjack), key exchange (e.g., FIPS 171), digital signature (e.g., DSA, RSA, ECDSA), and hash (e.g., SHA-1, SHA-256, SHA-384, SHA-512). Newer standards shall be recommended as they become available.

The Contractor shall ensure that all user interface services (e.g., web services) are physically or logically separated from data storage and management services (e.g., database management systems). Separation may be accomplished through the use of different computers, different CPUs, different instances of the operating system, different network addresses, combinations of these methods, or other methods as appropriate.

The Contractor shall not use Binary or machine executable public domain software products and other software products with limited or no warranty, such as those commonly known as freeware or shareware in the design/development of DHCS systems unless they are necessary for mission accomplishment, there are no alternative IT solutions available, and approved by the COR. Such products shall be assessed for cybersecurity impacts, and shall be required to be approved for use by the JMIS DAA. This requirement is due to the fact that such software products are difficult or impossible to review, repair, or extend, given that the Government does not have access to the original source code and there is no owner who could make such repairs on behalf of the Government.

The Contractor shall document all Ports, Protocols, and Services (PPS) traversing DOD networks specific to the electronic communications of DHCS-owned Contractor-managed systems. PPS documentation shall identify the Port, Protocol, Service, Source IP address, Destination IP address, and description of communication. PPS detail shall be included as a sub-section of deliverable "x" Interface Control Document (ICD). Contractors shall follow all current DOD and Defense Information Systems Agency (DISA) standards and requirements for acceptable Ports, Protocols, and Services. Any requests for exception to using the current DISA Ports, Protocols, and Services standards requires an request for exception sent through the ISSM to the DAA.

The Contractor shall ensure that all appointments to required CS roles, e.g., ISSM/ISSO, are established in writing, to include assigned duties and appointment criteria such as training, security clearance, and IT-designation.

The Contractor shall ensure that a Security Management Plan (SMP) is established **(Deliverable 20)** that describes the technical, administrative, and procedural IA program and policies that govern the DHCS-owned, Contractor-managed information system, and identifies all CS personnel and specific CS requirements and objectives (e.g., requirements for data handling or dissemination, system redundancy and backup, or emergency response).

The Contractor shall ensure compliance with DoD 8570.1 and DOD 8570.01_M. The Contractor shall provide a list of all contract personnel requiring system privilege level access. The Contractor shall define personnel into Information Assurance Technical (IAT) and Information Assurance Management

(IAM) categories per DOD 8570.01-M: IAT and IAM categories shall be further broken into privilege levels I, II, and III.

The Contractor shall ensure that all personnel identified as requiring privilege level access to computers, systems, and networks are appropriately certified in accordance with the approved programs specified in DoD 8570.01-M. The Contractor shall only provide privileged access to those approved by the COR. Personnel requiring privileged access who does not meet the requirements of DoDI 8570.01-M shall be supervised by an appropriately certified and approved individual. Supervision shall only be approved for six months from date of contract. Those persons not certified within the allotted time shall not be approved for privileged access past that time.

The Contractor shall ensure that appropriate certifications are identified as a condition of employment for new employees. The Contractor shall ensure that new employees acknowledge and agree to obtain the appropriate certification for the position to be filled within six months of employment.

The Contractor shall ensure that all personnel requiring privileged computer, system or network access have completed and signed an INFORMATION SYSTEM PRIVILEGED ACCESS AGREEMENT AND ACKNOWLEDGEMENT OF RESPONSIBILITIES.

The Contractor shall isolate their security support structure by means of partitions, domains, etc., including control of access to, and integrity of, hardware, software, and firmware that perform security functions. The security support structure shall maintain separate execution domains (e.g. address spaces) for each executing process.

The Contractor shall ensure that all DHCS-owned Contractor-managed systems' initialization, shutdown, and aborts are configured to ensure that the system remains in a secure state. The Contractor shall document testing procedures to validate this condition and shall periodically run them at the direction of the DHCS to ensure the integrity of the system state.

The Contractor shall ensure that a current and comprehensive baseline inventory of all software (SW) (to include manufacturer, type, and version and installation manuals and procedures) required to support DHCS-owned, Contractor-managed information system operations is provided to the DHCS CCB and is maintained as part of the C&A documentation. A backup copy of the inventory is stored in a fire-rated container or otherwise not collocated with the original. Contractors designing, developing or operating DoD ISs shall comply with the requirements of the DoD Information Assurance (IA) program as promulgated in DoDI 8500.1 Cybersecurity, March 14, 2014 and NIST Publication 800-53 Rev 4, April 30, 2013.
Contractor Information Systems (IS)/networks that are involved in the operation of systems in support of the DoD MHS shall operate in accordance with controlling laws, regulations, and DOD policy.

5.7 Identification and Authentication
The Contractor shall ensure that where PKI is used within the architecture of DHCS-owned Contractor-managed systems/networks, Symmetric Keys are produced, controlled and distributed using NSA-approved key management technology and processes. Asymmetric Keys shall be produced, controlled and distributed using DoD PKI Class 3 or Class 4 certificates and hardware security tokens that protect the user's private key.

The Contractor shall ensure that Identification and authentication is accomplished using the DoD PKI Class 3 or 4 certificate and hardware security token (when available) or an NSA-certified product.

The Contractor shall ensure that all group authenticators for access to DHCS-owned Contractor-managed assets are used only in conjunction with an individual authenticator. Any use of group authenticators not based on the DOD PKI must be explicitly approved by the appropriate Authorizing Official (AO).

The Contractor shall develop procedures for assigning group accounts and distributing individual authenticators. These procedures shall provide specific information necessary to ensure that those requesting access to sensitive information are identified to be whom they claim.

The Contractor shall maintain a list of all users and their assigned groups; this list shall be presented to the DHCS immediately upon request.

The Contractor shall ensure that access to DHCS-owned Contractor-managed assets is gained through the presentation of an individual identifier (e.g., a unique token or user login ID) and password. For systems utilizing a logon ID as the individual identifier, passwords shall, at a minimum:

- Passwords must be at least 15 characters long
- Passwords must contain a mix of upper case letters, lower case letters, numbers, and special characters
- When a password is changed, the user must not be able to use personal information such as names, telephone numbers, account names, or dictionary words
- Passwords must expire after 60 calendar days
- The user must not be able to reuse any of their previous 10 passwords
- The user must not be able to change passwords more than once a day, except in the case of an administrator or privileged user. Privileged users may be required to reset user's forgotten passwords and the ability to change passwords more than once per day
- When a password is changed, the new password must differ from the previous password by at least four characters
- (APP3320.1: CAT II) The Designer will ensure the application has the capability to require account passwords having a minimum of 15 alphanumeric characters in length.
- (APP3320.2: CAT II) The Designer will ensure the application has the capability to require account passwords contain a mix of upper case letters, lower case letters, numbers, and special characters.
- (APP3320.3: CAT II) The Designer will ensure the application has the capability to require account passwords be changed every 60 calendar days or more frequently.
- (APP3320.4: CAT II) The Designer will ensure passwords do not contain personal information such as names, telephone numbers, account names, or dictionary words.
- (APP3320.5: CAT II) The Designer will ensure the application has the capability to limit reuse of account passwords within the last 10 password changes.
- (APP3320.6: CAT II) The Designer will ensure the application has the capability to limit user changes to their account passwords once every 24 hours with the exception of privileged or administrative users.
- (APP3320.7: CAT II) The Designer will ensure the application has the capability to require new account passwords differ from the previous password by at least four characters when a password is changed.

5.8 Enclave and Computing Environment

The Contractor shall ensure that access control mechanisms exist to validate that all DHCS-owned Contractor-managed system data is accessed and changed only by authorized personnel.

The Contractor shall record in transaction logs, all access and changes to the data and shall review them periodically or immediately upon system security events. The Contractor shall ensure that change threats from code or system problems are included, and must provide documented procedures for verification.

The Contractor shall ensure that all privileged user accounts are established and administered in accordance with a role-based access scheme that organizes all system and network privileges into roles (e.g., key management, network, system administration, database administration, web administration).

The Contractor shall identify all privileged role assignments and shall report those assignments quarterly and at the request of the COR.

The Contractor shall ensure that all DHCS-owned Contractor-managed systems are configured in accordance with the most current DoD Information Systems Agency (DISA) Security Technical Implementation Guidance (STIG).

The Contractor shall ensure change controls for software development are in place to prevent unauthorized programs or modifications to programs from being implemented. Change controls include review and approval of application change requests and technical system features to assure that changes are executed by authorized personnel and are properly implemented.

The Contractor shall ensure good engineering practices with regards to the integrity mechanisms of COTS, GOTS, and custom developed solutions are implemented for incoming and outgoing files, such as parity checks and cyclic redundancy checks (CRCs).

The Contractor shall provide mechanisms to assure the integrity of all transmitted information (including labels and security parameters) and to detect or prevent the hijacking of a communication session (e.g., encrypted or covert communication channels).

The Contractor shall ensure that the contents of all DHCS-owned Contractor-managed systems' audit trails are protected against unauthorized access, modification, or deletion. The Contractor shall ensure that permissions for access to this information are limited to those Administrators and privileged users agreed to by the DHCS.

The Contractor shall ensure that access to all DOD information is determined by both its classification and user need-to-know. Need-to-know is established by the Information Owner and enforced by discretionary or role-based access controls.

The Contractor shall ensure that access controls are established and enforced for all shared or networked file systems and internal websites, whether classified, sensitive, or unclassified. All internal classified, sensitive, and unclassified websites are organized to provide at least three distinct levels of access:

- Open access to general information that is made available to all DOD authorized users with network access. Access does not require an audit transaction.
- Controlled access to information that is made available to all DOD authorized users upon the presentation of an individual authenticator. Access is recorded in an audit transaction.
- Restricted access to need-to-know information that is made available only to an authorized community of interest. Authorized users must present an individual authenticator and have either a demonstrated or validated need-to-know.

Private web servers are those web servers that restrict access by any means. The Contractor shall ensure access to Private Web Servers is performed through the use of DoD Public Key Infrastructure (PKI) certificates. Access to private web servers within the DOD shall be restricted to individuals with a valid DOD certificate. All access to need-to-know information and all failed access attempts shall be recorded in audit transactions.

The Contractor shall ensure that all DHCS-owned Contractor-managed systems' audit records include:

- User ID.
- Successful and unsuccessful attempts to access security files.
- Date and time of the event.
- Type of event.
- Success or failure of event.
- Successful and unsuccessful logons.
- Denial of access resulting from excessive number of logon attempts.
- Blocking or blacklisting a user ID, terminal or access port and the reason for the action.
- Activities that might modify, bypass, or negate safeguards controlled by the system.

If required by the DHCS, the Contractor shall ensure that NIST-certified cryptography is used to encrypt stored sensitive information.

The Contractor shall ensure that successive logon attempts to DHCS-owned Contractor-managed assets/systems are controlled using one or more of the following:

- Access is denied after multiple unsuccessful logon attempts.
- The number of access attempts in a given period is limited.
- A time-delay control system is employed.
- If the system allows for multiple-logon sessions for each user ID, the system shall provide a capability to control the number of logon sessions.

The Contractor shall ensure that access procedures are identified and provided to the DHCS. Access procedures shall enforce the principles of separation of duties and "least privilege". Access to privileged accounts of DHCS-owned Contractor-managed systems is limited to privileged users previously identified to the DHCS. Use of privileged accounts shall be limited to privileged functions; that is, privileged users use non-privileged accounts for all non-privileged functions. This control is in addition to an appropriate security clearance and need-to-know authorization. Specific procedures outline the specific requirements when handling PHI data.

The Contractor shall ensure that DHCS-owned Contractor-managed information and information systems that store, process, transit, or display data in any form or format that is not approved for public release comply with all requirements for marking and labeling contained in policy and guidance documents, such as DOD 5200.1R. Markings and labels clearly reflect the classification or sensitivity level, if applicable, and any special dissemination, handling, or distribution instructions.

The Contractor shall ensure that all authorizations to the information contained within an object are able to be revoked prior to initial assignment, allocation, or reallocation to a subject from the system's pool of unused objects. The Contractor shall ensure that no information, including encrypted representations of information, produced by a prior subject's actions is available to any subject that obtains access to an object that has been released back to the system. The Contractor shall ensure there is absolutely no residual data from the former object.

The Contractor shall ensure that all users of DHCS-owned Contractor-managed assets are warned that they are entering a Government information system, and are provided with appropriate privacy and security notices to include statements informing them that they are subject to monitoring, recording and auditing.

The Contractor shall develop/deliver a comprehensive account management process that once implemented shall ensure that only authorized users can gain access to DHCS-owned Contractor-managed workstations, applications, and networks and that individual accounts designated as inactive, suspended, or terminated are promptly deactivated. This process shall outline the procedures necessary to ensure that the privileged user is immediately advised when an account is no longer needed or should be terminated. The Contractor shall include in this process document, methods necessary to prevent duplicated user accounts.

The Contractor shall maintain any development environments in accordance with DHA Cybersecurity CS best practices and operational requirements. During product development for the Government, the Contractor shall ensure that all CS mitigation strategies have been applied to the development environment prior to any Government data being loaded onto any assets or software for testing or delivery.

5.9 Physical and Environmental

The Contractor shall ensure that all DHCS-owned Contractor-managed documents, equipment, and machine-readable media containing sensitive data are cleared and sanitized before being released outside of the Department of Defense according to DoD 5200.1-R and ASD (C3I) Memorandum, dated June 4, 2001, subject: "Disposition of Unclassified DoD Computer Hard Drives." Contractors shall follow the DOD standards, procedures, and use approved products to dispose of unclassified hard drives and other electronic media, as appropriate, in accordance with DOD Memorandum "Disposition of Unclassified Computer Hard Drives," June 4, 2001. Contractors are required to also follow DoD guidance on sanitization of other internal and external media components in DODI 8500.2 "Information Assurance (IA) Implementation," 6 Feb 2003 and DoD 5220.22-M "Industrial Security Program Operating Manual (NISPOM)," (Chapter 8). The Contractor shall implement procedures that address final disposition of PHI and/or the electronic media on which it is stored. The Contractor shall include approved methods of destruction to ensure PHI cannot be accessed once the media leaves their possession. The Contractor shall ensure that all PHI is removed from media prior to making it available for re-use within or outside of the DOD. The Contractor shall ensure that log documentation exists that indicates the release of equipment and identifies that it has been cleared, and sanitized.

The Contractor shall ensure that devices that display or output sensitive information in human-readable form are positioned to deter unauthorized individuals from reading the information. The Contractor shall ensure that every physical access point to facilities housing workstations that process or display sensitive information is controlled during working hours and guarded or locked during non-work hours.

5.10 Continuity

The Contractor shall ensure that back-up copies of the operating system and other critical software associated with DHCS-owned Contractor-managed systems are stored in a fire rated container or otherwise not collocated with the operational software. The Contractor shall ensure that recovery procedures and technical system features exist to ensure that recovery is done in a secure and verifiable manner. Circumstances that can inhibit a trusted recovery are documented and appropriate mitigating procedures have been put in place.

5.11 Vulnerability and Incident Management

The Contractor shall implement a comprehensive vulnerability management process that includes the systematic identification and mitigation of software and hardware vulnerabilities associated with DHCS-owned, Contractor-managed systems and their supporting networks. Wherever system capabilities permit, mitigation is independently validated through inspection and automated vulnerability assessment or state management tools. The Contractor shall ensure that approved vulnerability assessment tools have been acquired, personnel have been appropriately trained, procedures have been developed, and regular internal and external assessments are conducted. For improved interoperability, preference is given to tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention and use the Open Vulnerability Assessment Language (OVAL) to test for the presence of vulnerabilities.

The Contractor shall ensure that all vulnerability management processes and procedures are developed and coordinated through DHCS and that it integrates with all CM and release management processes.
IA mitigation strategies include security updates, service packs, and changes to operating procedures as physical and cyber vulnerabilities are detected. Operating system, routers, servers, development platforms and the application being delivered to the Government shall be in compliance with all known applicable Department of Defense Computer Emergency Response Team (DoD-CERT) Alert, Bulletin, and Technical Advisory Notices published during the past 36 months.

5.12 Enterprise Architecture (EA)

5.12.1 References

The contractor shall comply with terms indicated in current versions of below laws, guidance, policies of DoD, MHS and other guidance defined by DHCS Program Offices:

Architecture/Repositories

- DoD Architecture Framework (DoDAF) Version 2.0, May 28, 2009
- DOD Information Technology Standards Registry (DISR), Version 09-2.0, July 30, 2009
- TRICARE Management Activity – Military Health System Enterprise Architecture version 6.0

Business Transformation

- Deputy Under Secretary of Defense for Financial Management and the Deputy Under Secretary of Defense for Business Transformation Memorandum, "Release of New and Updated Department of Defense Business system Investment Review Related Guidance," April 11, 2006

General

- DoDD 5000.1 Defense Acquisition System, May 12, 2003
- DoDI 5000.2 Operation of the Defense Acquisition System, May 12, 2003
- DoDD 8000.1 Management of DoD Information Resources and Information Technology, March 20, 2002 Change 1
- Joint Vision 2020, 7 "Future Warfare," June 2000
- Office of Management and Budget (OMB) Circular NO. A-130: Management of Federal Information Resources, November 28, 2000
- Secretary of Defense Memorandum, "Implementation of Subdivision E of the Clinger Cohen Act of 1996 (Public Law 104-106)," June 2, 1997
- Department of Defense policies, Parts 600-799, Title 21, Code of Federal Regulations (21 CFR, PARTS 600-799)
- Defense Acquisition Guidebook, Policies, Directives, Regulations, Laws

Global Information Grid (GIG)/Net-Centricity

- DoDD 8100.1 Global Information Grid Overarching Policy, September 19, 2002
- Global Information Grid (GIG) Capstone Requirements Document, 5 JROCM 134-01, August 30, 2001
- Global Information Grid (GIG) Architecture Version 2.0, August 2003
- DoD CIO Memorandum, "Global Information Grid Enterprise Services (GIG ES): Transforming to a Net-Centric Environment—President's Budget FY 2006-2011," July 30, 2004
- DoD Deputy CIO, Information Management Memorandum, "Department of Defense (DoD) Net-Centric Data Strategy
- DoDD 8320.2 Data Sharing in a Net-Centric Department of Defense, December 2, 2004
- DoD Guidance 8320.02-G Guidance for Implementing Net-Centric Data Sharing, April 12, 2006

Integration & Interoperability

- CJCSI 3010.02B, Joint Operations Concepts Development Process (JOpsC-DP), 27 January 2006
- CJCSI 3100.01A, Joint Strategic Planning System, 1 September 1999 (updated 12 Sep 2003)
- CJCSI 3170.01G – Joint Capabilities Integration and Development System, 1 March 2009
- Manual for the Operation of the Joint Capabilities Integration and Development System (JCIDS) - Updated February 2009
- CJCSI 6212.01D, Interoperability and Supportability of Information Technology and National Security Systems, 8 March 2006
- CJCSI 8501.01A, Chairman of the Joint Chiefs of Staff, Combatant Commanders, and Joint Staff Participation in the Planning, Programming, Budgeting, and Execution System, 3 December 2004
- DoD Directive 7045.20, Capability Portfolio Management, September 25, 2008

Laws

- Public Law 104-106: Clinger-Cohen Act of 1996, February 10, 1996
- Health Insurance Portability and Accountability Act, 1996
- Public Law 93-579: Privacy Act of 1974
- Federal Information Security Management Act of 2002
- Public Law 104-113: National Technology Transfer and Advancement Act of 1995. 104th Congress, March 7, 1996

Security/Information Assurance/Technology

- DoDD 4630.5 Interoperability and Supportability of Information Technology (IT) and National Security systems (NSS), May 5, 2004
- DoDD 8100.2, Use of Commercial Wireless Devices and Services in the DOD Global Information Grid, April 14, 2004
- DoDD 8500.1, Information Assurance, October 24, 2002
- DoDD 8500.2, Information Assurance (IA) Implementation, February 6, 2003
- DoDI 4630.8 Procedures for Interoperability and Supportability of Information Technology (IT) and National Security systems (NSS), June 30, 2004
- Interim DOD Certification and Accreditation Process Guidance, July 6, 2006.
- DoD CIO Memo "Internet Protocol Version," Augut 16, 2005
- CJCSI 6212.01D Interoperability and Supportability of Information Technology and National Security systems (NSS), March 8, 2006

- NSTISSP No. 11, 4 National Policy Governing Information Assurance and Information Assurance Enabled Information Technology Products, January 2000
- EIA-649-B, National Consensus Standard for Configuration Management, April 2011
- GEIA-HB-649, Implementation Guide for Configuration Management, October 2005

Reference URLs

- http://www.whitehouse.gov/omb/e-gov/fea/ (Federal Enterprise Architecture Security and Privacy Profile)
- http://www.ipv6.com/articles/military/Military-and-IPv6.htm

- http://www.dod.mil/pubs

5.12.2 MHS Enterprise Architecture Requirements -- General

Architecture Guidance

- The Contractor shall adhere to goals, standards, constraints, guidelines, architectural products, and processes established and approved by the MHS Enterprise Architecture or higher levels of authority. These products will be available as Government Furnished Information (GFI) from the MHS Chief Architect via the DHCS Architecture team upon award.
- The Contractor shall ensure that products and services (deliverables) are aligned and compliant with the current MHS IM/IT Strategic Plan and Principles, MHS Enterprise Architecture.
- The Contractor shall employ strategies, technical solutions and project plans that support the DoD Net-Centric Service Oriented Architectures.

5.12.3 Documentation of Virtual Images

For a Contractor that is providing the Government with new server or workstation capability based on Microsoft Windows, LINUX or Sun Solaris x86 based platforms, the Government requires that the Contractor provide a copy of the server, as a VMware VM, in the same configuration as it would be deployed to the field with all DISA STiGs applied and software installed and functioning. This submission to the Government shall be in accordance with the DHCS CM Product Intake and Distribution guidance.

The Government requests a document with the base configuration of the VM, to include:

- Number of virtual processors
- Memory requirements of the VM
- Number of virtual network adapters assigned to the VM
- Any special network configuration requirements
- If there are multiple Virtual Disks assigned to the VM list them and define which drive letters are assigned to each one
- Administrative username and passwords for the VM

In addition to this document, the VMX and VMDK files associated with the VM should be transferred via SFTP or SCP to the DHCS lab environment.

5.12.4 Internet Protocol version 6 (IPv6)

The Contractor shall provide COTS solutions that are IPv6 capable. An IPv6 capable system or product shall be capable of receiving, processing, transmitting and forwarding IPv6 packets and/or interfacing with other systems and protocols in a manner similar to that of IPv4. Specific criteria to be deemed IPv6 capable are:

- Conformance to the DoD Information Technology Standards Repository (DISR) developed DoD IPv6 Standards Profile. Systems being developed, procured or acquired shall comply with the Global Information Grid Architecture and DISR standard IPv6 Capable definition. An IPv6 Capable system must meet the IPv6 base requirements defined in the "DoD IPv6 Standards Profile v1.0" dated June 1, 2006 available from the DISR.
- Maintenance of interoperability with IPv4. Systems being developed, procured or acquired shall maintain interoperability with IPv4 systems/capabilities. Systems should implement IPv4/IPv6dual-stack and should also be built to determine which protocol layer to use depending on the destination host it is attempting to communicate with or establish a socket with. If either protocol is possible, systems should employ IPv6.
- Evidence of a migration path and commitment to upgrade all applications and product features to IPv6.
- Availability of Contractor/vendor IPv6 technical support for system development, implementation and management.

DoD IPv6 security guidelines, standards, and solutions shall be utilized and adhered to when available. Currently, DoD IPv6 Information Assurance (IA) guidance is available from the DoD IPv6 Transition Office (DITO).

6.0 OTHER TERMS, CONDITIONS, AND PROVISIONS

6.1 Non-Disclosure /Non-Use Agreement – Deliverable 1

The Contractor shall ensure that the Non-Disclosure/Non-Use Agreement (PWS Attachment A) (**Deliverable 1**) is signed by all staff assigned to or performing on this Task order before performing any work, including all subcontractors and consultants. The Non-Disclosure/Non-Use Agreement shall be cosigned by a corporate official (Contractor Task Manager or higher). The Contractor shall also ensure that all staff understand and adhere to the terms of the non-disclosure statement, protecting the procurement sensitive information of the Government and the proprietary information of other Contractors. Assignment of any staff who have not executed this statement or failure to adhere to this statement shall constitute default on the part of the Contractor.

6.2 Information Assurance

6.2.1 Information Assurance General Security Requirements

The Contractor shall establish appropriate administrative, technical, and physical safeguards to protect any and all Government data, to ensure the confidentiality, integrity, and availability of Government data. As a minimum, this shall include provisions for personnel security, electronic security and physical security as listed in the sections that follow:

6.2.2 Personnel Security.

The Contractor shall comply with DoD Directive 8500.1, "Information Assurance (IA);" DoD Instruction 8500.2, "Information Assurance (IA) Implementation;" DoD Directive 5400.11, "DoD Privacy Program;" DoD 6025.18-R, "DoD Health Information Privacy Regulation;" and DoD 5200.2-R, "Personnel Security Program Requirements."

Contractor responsibilities for ensuring personnel security include, but are not limited to, meeting the following requirements:

- Follow the DHA Privacy Office guidelines for submittal of Automated Data Processor/Information Technology (ADP/IT) security clearances and ensure all Contractor personnel are designated as ADP/IT-I, ADP/IT-II, or ADP/IT-III where their duties meet the criteria of the position sensitivity designations. Contact the DHA Privacy Office for guidance on the appropriate ADP/IT levels for personnel on the contract. The DHA Privacy Office

procedures for personnel security will be provided by the Government. Initiate, maintain, and document personnel security investigations appropriate to the individual's responsibilities and required access to MHS Sensitive Information (SI).

- Immediately report to the DHA Privacy Office and deny access to any automated information system (AIS), network, or MHS SI information if a Contractor employee filling a sensitive position receives an unfavorable adjudication, if information that would result in an unfavorable adjudication becomes available, or if directed to do so by the appropriate Government representative for security reasons.
- Ensure that all Contractor personnel receive information assurance (IA) training before being granted access to DoD AISs/networks, and/or MHS SI information.

6.2.3 Electronic Security.

Contractor Information Systems (IS)/networks that are involved in the operation of systems in support of the DoD MHS shall operate in accordance with controlling laws, regulations, and DoD policy.

Contractors designing, developing or operating DoD ISs shall comply with the requirements of the DoD Information Assurance (IA) program as promulgated in DoDIA 8500.2IA Implementation, 6 February 2003.

Certification & Accreditation (C&A) requirements as promulgated in DoDI 8510.01 apply to all DoD and Contractor's IS/networks that receive, process, display, store or transmit DoD information. The Contractor shall comply with the C&A process for safeguarding SI. Certification is the determination of the appropriate level of protection required for IS/networks. Certification also includes a comprehensive evaluation of the technical and non-technical security features and countermeasures required for each system/network.

Accreditation is the formal approval by the Government to operate the Contractor's IS/networks in a particular security mode using a prescribed set of safeguards at an acceptable level of risk. In addition, accreditation allows IS/networks to operate within the given operational environment with stated interconnections; and with appropriate level of protection for the specified period.

The Contractor shall comply with C&A requirements, as specified by the Government that meet appropriate DoD Information Assurance requirements. The C&A requirements shall be met before the Contractor's system is authorized to access DoD data or interconnect with any DoD IS/network that receives, processes, stores, displays or transmits DoD data. The Contractor shall initiate the C&A process by providing the Contracting Officer, within 60 calendar days following task order start date, the required documentation necessary to receive an Approval to Operate (ATO). The Contractor shall make its IS/networks available for testing, and initiate the C&A testing four months (120 calendar days) in advance of accessing DoD data or interconnecting with DoD IS/networks. The Contractor shall ensure the proper Contractor support staff is available to participate in all phases of the C&A process. This includes, but is not limited to:

- Attending and supporting C&A meetings with the Government
- Supporting/conducting the vulnerability mitigation process
- Supporting the C&A Team during system security testing
- Contractors must confirm that their IS/networks are locked down prior to initiating testing.
- Confirmation of system lock down shall be agreed upon during the definition of the C&A boundary and be signed and documented as part of the System Security Authorization Agreement (SSAA)

- Locking down the system means that there shall be no changes made to the configuration of the system (within the C&A boundary) during the C&A process

Any re-configuration or change in the system during the C&A testing process will require a re-baselining of the system and documentation of system changes.

Vulnerabilities that have been identified by the Government as "must-fix" issues during C&A process must be mitigated according to the timeline identified by the Government Representative. C&A checklists are provided for complying DoD C&A requirements.
A request for a waiver to the C&A requirements may be submitted for temporary testing and other usual circumstances. A waiver request must be submitted, in writing, to the Designated Accrediting Authority (DAA). The request must include mitigation strategies that ensure adequate protection measures and security controls are in place (for example: air gapping a testing network).

Information Assurance Vulnerability Management (IAVM). The Contractor shall implement an information assurance vulnerability management program. The DoD IAVM program provides electronic security protections against known threats and vulnerabilities. The IAVM program requires the registration of DoD IS assets in the DoD Vulnerability Management System (VMS), which allows for the timely dissemination of critical vulnerability information. It also assists in the documentation and tracking of compliance, providing increased electronic security to MHS systems. As part of the program, the Contractor shall provide a primary and secondary point of contact in the VMS and to the MHS Information Assurance Vulnerability Alert (IAVA) Monitor. The point of contact shall provide, upon receipt of a vulnerability message, an acknowledgment of receipt via the VMS. The contactor shall thoroughly test all mitigations for the vulnerability, and upon applying the mitigation to the system, report compliance in the VMS. Receipt and compliance messages to the Government shall occur within the stipulated time window, as stated in the vulnerability message or in the VMS.

The Contractor shall ensure DoD IS assets that are under development are registered in the VMS and have all applicable electronic patches installed for the system (1) when the system is delivered to the Government, or (2) if the DoD IS assets are used to store or process Government data prior to delivery (such as when being used in testing and development).

Guidance regarding the requirement for IAVM is contained in the DoD Information Assurance Vulnerability Alert (IAVA) December 30, 1999 memorandum and Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01 provides additional reference information. Implementation is addressed in the Defense Information Systems Agency (DISA) IAVA Process Handbook, Version 2.1, June 11, 2002. An asset is any device on any DoD-owned, controlled or contracted IS or network, to include (but not limited to) workstations, servers, routing devices (routers, switches, firewalls), networked peripherals (e.g., network printers, portable electronic devices) and controlled interfaces (e.g., guards). A device is considered a node on a network if it has its own network identification (internet protocol (IP) and/or media access control address). The Defense Information System Agency's (DISA) VMS web enabled application is used to disseminate IA Vas Information Assurance Vulnerability Bulletins (IA VBs), and Information Assurance Technical Advisories down to the System Administrator (SA) and applicable personnel throughout the chain of command.

The Contractor shall maintain any development environments in accordance with DHA Information Assurance IA best practices and operational requirements. During product development for the Government, the Contractor shall ensure that all IA mitigation strategies have been applied to the development environment prior to any Government data being loaded onto any assets or software for testing or delivery.

IA mitigation strategies include security updates, service packs, and changes to operating procedures as physical and cyber vulnerabilities are detected. Operating system, routers, servers, development platforms and the application being delivered to the Government shall be in compliance with all known applicable Department of Defense Computer Emergency Response Team (DoD-CERT) Alert, Bulletin, and Technical Advisory Notices published during the past 36 months.

Disposing of Electronic Media. Contractors shall follow the DoD standards, procedures, and use approved products to dispose of unclassified hard drives and other electronic media, as appropriate, in accordance with DoD Memorandum "Disposition of Unclassified Computer Hard Drives", June 4, 2001. Contractors are required to also follow DoD guidance on sanitization of other internal and external media components in DODI 8500.2 "Information Assurance (IA) Implementation," 6 Feb 2003 and DoD 5220.22-M "Industrial Security Program Operating Manual (NISPOM)," (Chapter 8).

4 Ports, Protocols, and Services. Contractors shall follow all current DoD and Defense Information Systems Agency (DISA) standards and requirements for acceptable Ports, Protocols, and Services. Any requests for exception to using the current DISA Ports, Protocols, and Services standards requires an request for exception sent through the Program Manager to the DAA.

Public Key Infrastructure and Encryption. Contractors shall follow the DoD standards, policies, and procedures related to the use of Public Key Infrastructure (PKI) certificates and biometrics for positive authentication. Where interoperable PKI is required for the exchange of unclassified information between DoD and its Contractors, industry partners shall obtain all necessary certificates. Contractors must turn over to the Government all encryption keys for deployed systems, backdoor algorithms, and procedures for their use in remote support. Contractors must provide a written report detailing all of the above, prior to task order expiration, regardless of modifications or extensions.

6.2.4 Information Systems (IS)/Networks Physical Security

The Contractor shall employ physical security safeguards for IS/Networks involved in processing or storage of Government Data to prevent the unauthorized access, disclosure, modification, destruction, use, etc., and to otherwise protect the confidentiality and ensure use conforms with DoD regulations. In addition, the Contractor will support a Physical Security Audit performed by the Government of the Contractor's internal information management infrastructure. The MHS Physical Security Audit Matrix will be provided by the Government. The Contractor shall correct any deficiencies identified by the Government of the Contractor's physical security posture. The Contractor shall be required to follow all requirements in the MHS Information Assurance Policy. New MHS policies will be provided by the Government.

6.3 Enterprise Architecture

Refer to section 5.12.

6.4 Protection of Information

6.4.1 Dissemination of Information/Publishing

There shall be no dissemination or publication, except within and between the Contractor and any subcontractors or specified Integrated Product/Process Team (IPT) members who have a need to know, of information developed under this order or contained in the reports to be furnished pursuant to this order without prior written approval of the DHA TM or the Contracting Officer. DHA approval for publication

will require provisions which protect the intellectual property and patent rights of both DHA and the Contractor.

6.4.2 Contractor Employees

Contractor Identification:
The Contractor shall ensure that Contractor personnel identify themselves as Contractors when attending meetings, answering Government telephones, providing any type of written correspondence, or working in situations where their actions could be construed as official Government acts.

Attendance at Meetings:
Contractor personnel may be required to attend meetings or otherwise communicate with Government and/or other contract representatives to meet the requirements of this order. Contractor personnel shall make their Contractor status known during introductions.

Use of Military Rank by Contractor Personnel:
Contractor personnel, while performing in a Contractor capacity, are prohibited from using their retired or reserve component military rank or title in all written or verbal communications associated with the contract under which they provide services.

6.4.3 Personally Identifiable Information (PII) and Protected Health Information (PHI)

The DHA Privacy Office website at http://www.tricare.mil/tma/privacy contains guidance regarding Protected Health Information (PHI) and Personally Identifiable Information PII).

General Requirements Overview

Personally Identifiable Information (PII), Protected Health Information (PHI) and Federal Information Laws

This section addresses the Contractor's requirements under The Privacy Act of 1974 (Privacy Act), The Freedom of Information Act (FOIA), and The Health Insurance Privacy and Accountability Act (HIPAA) as set forth in applicable statutes, implementing regulations and DoD issuances. In general, the Contractor shall comply with the specific requirements set forth in this section and elsewhere in this Contract. The Contractor shall also comply with requirements relating to records management as described herein.

This Contract incorporates by reference the federal regulations and DoD issuances referred to in this Section. If any authority is amended or replaced, the changed requirement is effective when it is incorporated under contract change procedures. Where a federal regulation and any DoD issuance govern the same subject matter, the Contractor shall first follow the more specific DoD implementation unless the DoD issuance does not address or is unclear on that matter. DoD issuances are available at http://www.dtic.mil/whs/directives.

For purposes of this Section, the following definitions apply.

DoD Privacy Act Issuances means the DoD issuances implementing the Privacy Act, which are DoDD 5400.11 (2007 thru Change 1 September 1, 2011) and DoDM 5400.11 (*2014]*). *The foregoing sentence assumes that* DoDM 5400.11 *will be published before this Contract is executed. If that is not the case, then the reference should be to the current issuance, i.e. DoD 5400.11-R (2007).*

HIPAA Rules means, collectively, the HIPAA Privacy, Security, Breach and Enforcement Rules, issued by the U.S. Department of Health and Human Services (HHS) and codified at 45 CFR Part 160 and Part 164, Subpart E (Privacy), Subpart C (Security), Subpart D (Breach) and Part 160, Subparts C-D (Enforcement), as amended by the 2013 modifications to those Rules, 78 FR 5566-5702 (Jan. 25, 2013) (with corrections at 78 FR 32464 (June 7, 2013)). Additional HIPAA rules regarding electronic

transactions and code sets (45 CFR Part 162) are not addressed in this Section and are not included in the term HIPAA Rules.

DoD HIPAA Issuances means the DoD issuances implementing the HIPAA Rules in the DoD Military Health System (MHS). These issuances are DODI 6025.18 (2014), and DODI 8580.02 (2014). *The foregoing sentence assumes that DODI 6025.18 and DODI 8580.02 will be published before this Contract is executed. If those issuances are not published, then the references should be to the current issuances, i.e. DoD 6025.18-R (2003),* DODI 6025.18 (2009), *and DOD 8580.02-R (2007).*

DHA Privacy Office means the DHA Privacy and Civil Liberties Office. The DHA Privacy Office Chief is the HIPAA Privacy and Security Officer for DHA, including the National Capital Region Medical Directorate (NCRMD).

Service-Level Privacy Office means a privacy office of one of the military Services (Army, Navy, or Air Force). The Service-Level Privacy Offices have authority over Privacy Act and HIPAA compliance by the military Services.

Breach means actual or possible loss of control, unauthorized disclosure of or unauthorized access to PHI or other PII (which may include, but is not limited to PHI), where persons other than authorized users gain access or potential access to such information for any purpose other than authorized purposes, where one or more individuals will be adversely affected. The foregoing definition is based on the definition of breach in DoD Privacy Act Issuances as defined herein.

HHS Breach means a breach that satisfies the HIPAA Breach Rule definition of a breach in 45 CFR 164.402.

Records Management

When creating and maintaining official government records, the Contractor shall comply with all Federal requirements established by 44 USC Chapters 21, 29, 31, 33 and 35, and by 36 CFR, Chapter XII, Subchapter B – Records Management. The Contractor shall also comply with DoD Administrative Instruction No. 15 (DoD AI-15), “OSD Records and Information Management Program” (2013).

Health Insurance Portability and Accountability Act (HIPAA)

The Contractor shall comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) (P.L. 104-191) requirements, as well as the Department of Defense (DoD) 6025.18-R, "DOD Health Information Privacy Regulation”, January, 2003. This includes the Standards for Electronic Transactions, the Standards for Privacy of Individually Identifiable Health Information and the Security Standards. The Contractor shall also comply with all Applicable HIPAA-related rules and regulations as they are published and as Government requirements are defined (including identifiers for providers, employers, health plans, and individuals, and standards for claims Appendix transactions). Any rules and regulations that are published and/or requirements that are defined after the award date of this contract, that require expenditure of additional Contractor resources for compliance may be considered "changes" and will be subject to the changes clause under the contract.

Breach Response

In the event of a breach of PII/PHI by the Contractor, the Contractor shall follow the breach response requirements set forth in this paragraph, which are designed to satisfy both the Privacy Act and HIPAA as applicable. If a breach involves only PII, then the Contractor shall comply with DoD Privacy Act Issuance breach response requirements only; if a breach involves PHI (a subset of PII), then the Contractor shall comply with both Privacy Act and HIPAA breach response requirements. A breach involving PHI may or may not constitute an HHS Breach. If a breach is not an HHS Breach, then the Contractor has no HIPAA breach response obligations. In such cases, the Contractor must still comply with breach response requirements under the DoD Privacy Act Issuances.

If the DHA Privacy Office determines that a breach is an HHS Breach, then the Contractor shall comply with both the HIPAA Breach Rule and DoD Privacy Act Issuances, as directed by the Privacy Office, regardless of whether the breach occurs at DHA or at one of the Service components. If the Privacy Office determines that the breach does not constitute an HHS Breach, then the Contractor shall comply with DoD Privacy Act Issuances, as directed by the Privacy Office.

The following provisions of this paragraph set forth the Contractor's Privacy Act and HIPAA breach response requirements for DHA breaches, including but not limited to HHS breaches. For other breaches not involving the DHA Privacy Office (i.e., Privacy Act-only breaches occurring at a Service-level component), the Contractor shall follow the directions of the Service-Level Privacy Office.

The Contractor shall comply with all breach response requirements set forth in this paragraph. In general, for breach response, the Contractor shall report the breach to the government, assess the breach incident, notify affected individuals, and take mitigation actions as applicable. Because DoD defines "breach" to include possible (suspected) as well as actual (confirmed) breaches, the Contractor shall implement these breach response requirements immediately upon the Contractor's discovery of a possible breach.

Applicable DHA Privacy Office guidance available at: http://www.tricare.mil/tma/privacy/breach.aspx.

Systems of Records

In order to meet the requirements of the Privacy Act and the DoD Privacy Act Issuances, the Contractor shall identify to the DHA Contracting Officer (CO) systems of records that are or will be maintained or operated for DHA where records of PII collected from individuals are maintained and specifically retrieved using a personal identifier. Upon identification of such systems to the CO, and prior to the lawful operation of such systems, the Contractor shall coordinate with the DHA Privacy Office to complete systems of records notices (SORNs) for submission and publication in the *Federal Register* as coordinated by the Defense Privacy and Civil Liberties Office, and as required by the DoD Privacy Act Issuances.

Following proper SORN publication and Government confirmation of Contractor authority to operate the applicable system(s), the Contractor shall also comply with the additional systems of records and SORN guidance, in coordination with the DHA Privacy Office, regarding periodic system review, amendments, alterations, or deletions set forth by the DoD Privacy Act Issuances, Office of Management and Budget (OMB) Memorandum 99-05, and OMB Circular A-130. The Contractor shall promptly advise the DHA Privacy Office of changes in systems of records or their use that may require a change in the SORN.

The Contractor shall also comply and become familiar with the following FAR Clauses as part of their training:

- 52.224-1 Privacy Act Notification and 52-224-2 Privacy Act.

Privacy Impact Assessment (PIA)

The Contractor shall provide for the completion of a PIA for any applicable systems that collect, maintain, use or disseminate PII or PHI about members of the public, federal personnel, contractors, or in some cases foreign nationals. The Contractor shall establish practices that satisfy the requirements of DODI 5400.16, "DOD Privacy Impact Assessment (PIA) Guidance", February 12, 2009.

To begin the PIA process, the Contractor shall use the DoD-approved PIA Template, DD Form 2930. The Contractor shall use the DHA PIA Guide (http://www.tricare.mil/tma/privacy/downloads/TMAPrivacyImpactAssessmentGuide.pdf) to complete the DD Form 2930. The Contractor should send completed DD Form 2930s to the DHA Privacy Office for review and approval, with a copy to the CO.

Data Sharing Agreement (DSA)

(Applies if contract requirements involve PII/PHI or de-identified data that would be PII/PHI)

The Contractor shall consult with the DHA Privacy Office to determine if the Contractor must obtain a Data Sharing Agreement (DSA) or Data Use Agreement (DUA), when MHS data that is managed by DHA will be accessed, used, disclosed or stored, to perform the requirements of this Contract. The Contractor shall comply with requests for additional documentation by the DHA Privacy Board when requesting PHI for research.

In addition, the Contractor shall submit any research requests for MHS data that include PHI to the DHA Privacy Board in order to be reviewed for HIPAA compliance.

The Contractor shall comply with the permitted uses established in a DSA/DUA to prevent the unauthorized use and/or disclosure of any PII/PHI, in accordance with the HIPAA Rules and the DoD HIPAA Issuances. Likewise, the Contractor shall comply with the DoD Privacy Act Issuances.

To begin the data sharing request process, the Contractor shall submit a Data Sharing Agreement Application (DSAA) to the DHA Privacy Office. If the application is approved, the requestor shall enter into one of the following agreements, depending on the data involved:

- DSA for De-Identified Data
- DSA for PHI
- DSA for PII Without PHI
- Data Use Agreement for Limited Data Set.

DSAs are active for one year, or until the end of the current option year, whichever comes first. If the DSA will not be renewed, the Contractor shall provide a Certificate of Data Disposition (CDD) to the DHA Privacy Office.

Privacy Act and HIPAA Training

The Contractor shall ensure that its entire staff, including subcontractors and consultants that perform work on this Contract receive training on the Privacy Act, HIPAA, the Alcohol, Drug Abuse and Mental Health Administration (ADAMHA) Reorganization Act, 42 USC 290dd-2, and the ADAMHA implementing regulations, 42 CFR Part 2.

The Contractor shall ensure all employees and subcontractors supply a certificate of all training completion to the Contracting Officer's Representative (COR) within 30 calendar days of being assigned and on an annual basis based on the trainee's birth month thereafter.

HIPAA Business Associate Provisions

Business Associate – General Provisions

The Contractor meets the definition of Business Associate, and DHA meets the definition of a covered entity under the HIPAA Rules and the DoD HIPAA Issuances. Therefore, a Business Associate Agreement (BAA) between the Contractor and DHA is required to comply with the HIPAA Rules and the DoD HIPAA Issuances. This paragraph 8 serves as the required BAA. As a Business Associate, the Contractor shall comply with the HIPAA Rules and the DoD HIPAA Issuances applicable to a business associate performing under this Contract.

Catch-All Definition: The following terms used, but not otherwise defined in paragraph 8.1, shall have the same meaning as those terms have in the DoD HIPAA Issuances: Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices (NoPP), Protected Health Information (PHI), Required By Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information (Unsecured PHI), and Use.

The Contractor shall not use or further disclose PHI other than as permitted or required by the Contract or as Required by Law.

The Contractor shall use appropriate safeguards, and comply with the HIPAA Security Rule with respect to electronic PHI, to prevent use or disclosure of PHI other than as provided for by the Contract.

The Contractor shall report to DHA any breach of which it becomes aware, and shall proceed with breach response steps as required by Paragraph 9. With respect to electronic PHI, the Contractor shall also respond to any security incident of which it becomes aware in accordance with any Information Assurance provisions of this Contract. If at any point the Contractor becomes aware that a security incident involves a breach, the contractor shall immediately initiate breach response as required by paragraph 9.

In accordance with DODI 6025.18.and (2) DODI 8580.02, paragraph 1.i.(3) (corresponding to 45 CFR 164.502(e)(1)(ii)) and 164.308(b)(2), respectively), as applicable, the Contractor shall ensure that any subcontractors that create, receive, maintain, or transmit PHI on behalf of the Contractor agree to the same restrictions, conditions, and requirements that apply to the Contractor with respect to such PHI.

With respect to individual rights of access to PHI, the Contractor shall make available PHI in a designated record set to the individual or the individual's designee as necessary to satisfy DHA's obligations under the DoD HIPAA Issuances and the corresponding 45 CFR 164.524. If the Contractor intends to deny the individual's request, the Contractor shall forward it (within seven business days of receipt) to the CO. The CO shall make a determination within 20 calendar days (50 calendar days for justified delays) of the request. The CO shall notify the individual, with a copy to the Contractor, of any approved or denied access determinations and the reason for any denial. The individual may appeal the denial determination to the DHA Privacy Office.

The Contractor shall make any amendment(s) to PHI in a designated record set as directed or agreed to by DHA, or take other measures as necessary to satisfy DHA's obligations under the DoD HIPAA Issuances and the corresponding 45 CFR 164.526.

The Contractor shall maintain and make available to the Government the information required to provide an accounting of disclosures to the MHS or to the individual as necessary to satisfy DHA's obligations under the DoD HIPAA Issuances and the corresponding 45 CFR 164.528.

To the extent the Contractor is to carry out one or more of DHA's obligation(s) under the HIPAA Rules, the Contractor shall comply with the requirements of the HIPAA Rules.

The Contractor shall make its internal practices, books, and records available to the HHS Secretary for purposes of determining compliance with the HIPAA Rules.

Permitted Uses and Disclosures

General Use and Disclosure Provisions

The Contractor may only use or disclose PHI as necessary to perform the services set forth in this Contract or as required by law. The Business Associate is not permitted to de-identify PHI under DoD HIPAA Issuances or the corresponding 45 CFR 164.514(a)-(c), nor is it permitted to use or disclose de-identified PHI, except as provided by the Contract or directed by DHA. The Contractor agrees to use, disclose and request PHI only in accordance with the HIPAA Privacy Rule "minimum necessary" standard and corresponding DHA policies and procedures as stated in the DoD HIPAA Issuances. The Contractor shall not use or disclose PHI in a manner that would violate the DoD HIPAA Issuances or HIPAA Privacy Rules if done by the covered entity, except uses and disclosures for the Contractor's own management and administration and legal responsibilities or for data aggregation services as set forth in below paragraphs.

Specific Use and Disclosure Provisions

Except as otherwise limited in this Section, the Contractor may use PHI for the proper management and administration of the Contractor or to carry out the legal responsibilities of the Contractor. The foregoing authority to use PHI does not apply to disclosure of PHI, which is covered in the next paragraph.

Except as otherwise limited in paragraph 8.3, the Contractor may disclose PHI for the proper management and administration of the Contractor or to carry out the legal responsibilities of the Contractor, provided that disclosures are required by law, or the Contractor obtains reasonable assurances from the person to whom the PHI is disclosed that it will remain confidential and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person, and the person notifies the Contractor of any instances of which it is aware in which the confidentiality of the information has been breached.

Except as otherwise limited in this Section, the Contractor may use PHI to provide Data Aggregation services relating to DHA's health care operations.

Contractor Compliance with DHA Notices and Restrictions

DHA will provide the Contractor with the notice of privacy practices that DHA produces in accordance with the DoD HIPAA Issuances and the corresponding 45 CFR 164.520.

Upon notification by DHA of any changes in, or revocation of, permission by an Individual to use or disclose his or her PHI, the Contractor shall comply to the extent that such changes may affect the Contractor's use or disclosure of PHI.

Upon notification by DHA, the Contractor shall comply with any restriction on the use or disclosure of PHI that the Government has agreed to or is required to abide by under the DoD HIPAA Issuances or the corresponding 45 CFR 164.522 , to the extent that such restriction may affect Contractor's use or disclosure of PHI.

Permissible Requests by DHA

The Government will not request the Contractor to use or disclose PHI in any manner that would not be permissible under the HIPAA Rules or any applicable Government regulations (including without limitation, DoD HIPAA Issuances) if done by the Government, except for providing Data Aggregation services to the Government and for management and administrative activities of the Contractor as otherwise permitted by this Contract.

Termination

Effect of Noncompliance

Noncompliance by the Contractor (or any of its staff, agents, or subcontractors) with any requirement in these HIPAA Business Associate Provisions (paragraph 8) may subject the Contractor to termination under any applicable default or other termination provision of this Contract.

Effect of Termination

If this Contract has records management requirements, the Contractor shall handle such records in accordance with the records management requirements. If this Contract does not have records management requirements, the Contractor shall handle such records in accordance with paragraphs 8.6.2.2 and 8.6.2.3 below. If this Contract has provisions for transfer of records and PII/PHI to a successor contractor, or if DHA gives directions for such transfer, the Contractor shall handle such records and information in accordance with such Contract provisions or DHA direction.

If this Contract does not have records management requirements, except as provided in paragraph 8.6.2.3 below, upon termination of the Contract, for any reason, the Contractor shall return or destroy all PHI received from the Government, or created or received by the Contractor on behalf of the Government that the Contractor still maintains in any form. This provision shall apply to PHI that is in the possession of subcontractors or agents of the Contractor. The Contractor shall retain no copies of the PHI.

If this Contract does not have records management provisions and the Contractor determines that returning or destroying the PHI is infeasible, the Contractor shall provide to the Government notification of the conditions that make return or destruction infeasible. Upon mutual agreement of the Government and the Contractor that return or destruction of PHI is infeasible, the Contractor shall extend the protections of the Contract to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as the Contractor maintains such PHI.

Miscellaneous

Survival
The obligations of the Contractor under the "Effect of Termination" provision of this Paragraph 9 shall survive the termination of this Contract.

Interpretation
Any ambiguity in this Contract shall be interpreted in a manner to permit compliance with the HIPAA Rules and the DoD HIPAA Issuances.

Breach Response

In the event of a breach of PII/PHI by the Contractor, the Contractor shall follow the breach response requirements set forth in this paragraph, which are designed to satisfy both the Privacy Act and HIPAA as applicable. If a breach involves only PII, then the Contractor shall comply with DoD Privacy Act Issuance breach response requirements only; if a breach involves PHI (a subset of PII), then the Contractor shall comply with both Privacy Act and HIPAA breach response requirements. A breach involving PHI may or may not constitute an HHS Breach. If a breach is not an HHS Breach, then the Contractor has no HIPAA breach response obligations. In such cases, the Contractor must still comply with breach response requirements under the DoD Privacy Act Issuances.

If the DHA Privacy Office determines that a breach is an HHS Breach, then the Contractor shall comply with both the HIPAA Breach Rule and DoD Privacy Act Issuances, as directed by the Privacy Office, regardless of whether the breach occurs at DHA or at one of the Service components. If the Privacy Office determines that the breach does not constitute an HHS Breach, then the Contractor shall comply with DoD Privacy Act Issuances, as directed by the Privacy Office.

The following provisions of this paragraph set forth the Contractor's Privacy Act and HIPAA breach response requirements for DHA breaches, including but not limited to HHS breaches. For other breaches not involving the DHA Privacy Office (i.e., Privacy Act-only breaches occurring at a Service-level component), the Contractor shall follow the directions of the Service-Level Privacy Office.

The Contractor shall comply with all breach response requirements set forth in this paragraph. In general, for breach response, the Contractor shall report the breach to the government, assess the breach incident, notify affected individuals, and take mitigation actions as applicable. Because DoD defines "breach" to include possible (suspected) as well as actual (confirmed) breaches, the Contractor shall implement these breach response requirements immediately upon the Contractor's discovery of a possible breach.

Reporting Provisions

The Contractor shall report the breach within one hour of discovery to the US Computer Emergency Readiness Team (US CERT), and, within 24 hours of discovery, to the DHA Privacy Office, and the other parties set forth below. The Contractor is deemed to have discovered a breach as of the time a breach (suspected or confirmed) is known, or by exercising reasonable diligence would have been known, to any person (other than the person committing it) who is an employee, officer or other agent of the Contractor.

The Contractor shall submit the US-CERT report using the online form at https://forms.us-cert.gov/report/. Before submission to US-CERT, the Contractor shall save a copy of the on-line report. After submission, the Contractor shall record the US-CERT Reporting Number. Although only limited

information about the breach may be available as of the one hour deadline for submission, the Contractor shall submit the US-CERT report by the deadline. The Contractor shall e-mail updated information as it is obtained, following the instructions at http://www.us-cert.gov/pgp/email.html. The Contractor shall provide a copy of the initial or updated US-CERT report to the DHA Privacy Office and the applicable Service-Level Privacy Office, if requested by either. Contractor questions about US-CERT reporting shall be directed to the DHA Privacy Office, not the US-CERT office.

The Contractor report to DHA due within 24 hours shall be submitted by completing the New Breach Reporting Form DD 2959 at the Breach Response page on the DHA Privacy Office web site and emailing that form to the DHA Privacy Office, the DHA CO and COR, and the DHA Program Office (or Service-Level Privacy Office) applicable to the Contractor. For the applicable Program Office, the Contractor shall e-mail the notice to its usual Point of Contact (POC) unless the POC specifies another addressee for breach reporting. Encryption is not required, because Breach Report Forms should not contain PII/PHI. The email address for notices to the DHA Privacy Office is provided at the Privacy Office website breach response page. If electronic mail is not available, telephone notification is also acceptable, but all notifications and reports delivered telephonically must be confirmed by email as soon as technically feasible.

If multiple beneficiaries are affected by a single event or related set of events, then a single reportable breach may be deemed to have occurred, depending on the circumstances. The Contractor shall inform the DHA Privacy Office as soon as possible if it believes that "single event" breach response is appropriate; the DHA Privacy Office will determine how the Contractor shall proceed and, if appropriate, consolidate separately reported breaches for purposes of Contractor report updates, beneficiary notification, and mitigation. The corresponding CDRL, entitled "Breach Report", provides further guidance on completing and updating the Breach Report Form.

When a Breach Report Form initially submitted is incomplete or incorrect due to unavailable information, or when significant developments require an update, the Contractor shall submit a revised form or forms, stating the updated status and previous report date(s) and showing any revisions or additions in red text. Examples of updated information the Contractor shall report include, but are not limited to: confirmation on the exact data elements compromised, the root cause of the incident, and any mitigation actions to include, sanctions, training, incident containment, follow-up, etc. The Contractor shall submit these report updates promptly after the new information becomes available. Prompt reporting of updates is required to allow the DHA Privacy Office to make timely final determinations on any subsequent notifications or reports. The Contractor shall provide updates to the same parties as required for the initial Breach Report Form. The Contractor is responsible for reporting all information needed by the DHA Privacy Office to make timely and accurate determinations on reports to HHS as required by the HHS Breach Rule and reports to the Defense Privacy and Civil Liberties Office as required by DoD Privacy Act Issuances.

In the event the Contractor is uncertain on how to apply the above requirements, the Contractor shall consult with the CO, who will consult with the Privacy Office as appropriate when determinations on applying the above requirements are needed.

Individual Notification Provisions

If the Privacy Office determines that individual notification is required, the Contractor shall provide written notification to individuals affected by the breach as soon as possible, but no later than 10 business days after the breach is discovered and the identities of the individuals are ascertained. The 10 business day period begins when the Contractor is able to determine the identities (including addresses) of the individuals whose records were impacted.

The Contractor's proposed notification to be issued to the affected individuals shall be submitted to the parties to which reports are submitted under paragraph 9.1 for their review, and for approval by the DHA Privacy Office. Upon request, the Contractor shall provide the DHA Privacy Office with the final text of

the notification letter sent to the affected individuals. If different groups of affected individuals receive different notification letters, then the Contractor shall provide the text of the letter for each group. (PII shall not be included with the text of the letter(s) provided.) Copies of further correspondence with affected individuals need not be provided unless requested by the Privacy Office. The Contractor's notification to the individuals, at a minimum, shall include the following:
—The individual(s) must be advised of what specific data was involved. It is insufficient to simply state that PII has been lost. Where names, Social Security Numbers (SSNs) or truncated SSNs, and Dates of Birth (DOBs) are involved, it is critical to advise the individual that these data elements potentially have been breached.

—The individual(s) must be informed of the facts and circumstances surrounding the breach. The description should be sufficiently detailed so that the individual clearly understands how the breach occurred.

—The individual(s) must be informed of what protective actions the Contractor is taking or the individual can take to mitigate against potential future harm. The notice must refer the individual to the current Federal Trade Commission (FTC) web site pages on identity theft and the FTC's Identity Theft Hotline, toll-free: 1-877-ID-THEFT (438-4338); TTY: 1-866-653-4261.

—The individual(s) must also be informed of any mitigation support services (e.g., one year of free credit monitoring, identification of fraud expense coverage for affected individuals, provision of credit freezes, etc.) that the Contractor may offer affected individuals, the process to follow to obtain those services and the period of time the services will be made available, and contact information (including a phone number, either direct or toll-free, e-mail address and postal address) for obtaining more information.

Contractors shall ensure any envelope containing written notifications to affected individuals are clearly labeled to alert the recipient to the importance of its contents, e.g., "Data Breach Information Enclosed", and that the envelope is marked with the identity of the Contractor and/or subcontractor organization that suffered the breach. The letter must also include contact information for a designated POC to include, phone number, email address, and postal address.

If the Contractor determines that it cannot readily identify, or will be unable to reach, some affected individuals within the 10 business-day period after discovering the breach, the Contractor shall so indicate in the initial or updated Breach Report Form. Within the 10 business-day period, the Contractor shall provide the approved notification to those individuals who can be reached. Other individuals must be notified within 10 business days after their identities and addresses are ascertained. The Contractor shall consult with the DHA Privacy Office, which will determine the media notice most likely to reach the population not otherwise identified or reached. The Contractor shall issue a generalized media notice(s) to that population in accordance with Privacy Office approval.

The Contractor shall, at no cost to the government, bear any costs associated with a breach of PII/PHI that the Contractor has caused or is otherwise responsible for addressing.

Breaches are not to be confused with security incidents (often referred to as cyber security incidents when electronic information is involved), which may or may not involve a breach of PII/PHI. In the event of a security incident not involving a PII/PHI breach, the Contractor shall follow applicable DoD Information Assurance requirements under its contract. If at any point the Contractor finds that a cyber-security incident involves a PII/PHI breach (suspected or confirmed), the Contractor shall immediately initiate the breach response procedures set forth below. The Contractor shall also continue to follow any required cyber security incident response procedures to the extent needed to address security issues, as determined by DoD/DHA.

6.4.4 Protection of Human Subjects and Adherence to Ethical Standards in Department of Defense (DoD)-Supported Research

Not Applicable

6.4.5 Public Key Infrastructure Authentication and Encryption.

Contractors shall follow the DoD standards, policies, and procedures related to the use of Public Key Infrastructure (PKI) certificates and biometrics for positive authentication including authentication to DoD private web servers or applications. Where interoperable PKI is required for the exchange of unclassified information, including the encryption of e-mail containing sensitive information, between DoD and its Contractors, industry partners shall obtain all necessary certificates if they are not eligible for a DoD Common Access Card. (refer to http://iase.disa.mil/pki/eca/ and http://www.cac.mil/)

6.5 Access Requirements

6.5.1 Contractor access to HA/TMA Network/DoD Systems

The Contractor will require access to the HA/TMA Network/DoD Systems to perform work under this task.

6.5.2 Contractor access to classified information

NA.**6.6 Data Rights**

The Government will retain rights to all data produced in the course of developing, deploying, training, using and supporting TMA or other federal agencies that utilize this order.

6.7 Organizational Conflict of Interest (OCI) Category

Contractor and subcontractor personnel performing work under this contract may receive, have access to or participate in the development of proprietary or source selection information (e.g., cost or pricing information, budget information or analyses, specifications or work statements, etc.) or perform evaluation services which may create a current or subsequent Organizational Conflict of Interests (OCI) as defined in FAR Subpart 9.5. After the original OCI disclosure, required by the RFQ, is submitted with the Contractor's quote, the Contractor shall continually monitor any actual or potential OCI occurring during the entirety of the performance of this task order. The Contractor shall notify the Contracting Officer immediately whenever it becomes aware that such access or participation may result in any actual or potential OCI and shall promptly submit a plan to the Contracting Officer to avoid or mitigate any such OCI. The Contractor's mitigation plan will be determined to be acceptable solely at the discretion of the Contracting Officer and in the event the Contracting Officer unilaterally determines that any such OCI cannot be satisfactorily avoided or mitigated, the Contracting Officer may affect other remedies as he or she deems necessary, including prohibiting the Contractor from participation in subsequent contracted requirements which may be affected by the OCI.

7.0 APPLICABLE DOCUMENTS AND DEFINITIONS

7.1. Compliance Documents and Reference Documents

The Contractor shall adhere, to the extent applicable to the Contractor's obligations, to the policy and procedures as outlined in the documentation indicated below. The Contractor shall also adhere to any laws, regulations, policies, procedures, and guidelines relevant to the specific tasks being performed in this DO.

- Defense Data Dictionary System (DDDS), 29 May 2002
- EIA-649A, "National Consensus Standard for Configuration Management"
- Health Insurance Portability and Accountability Act of 1996
- Health Insurance Portability and Accountability Act of 1996 (Privacy Rule) effective October 15, 2002

- Health Insurance Portability and Accountability Act of 1996 (Security Rule) effective April 21, 2003
- Privacy Act of 1974, (5 U.S.C. 552a eq. seq)
- DoD 5000 Series, current version
- MHS Information Assurance (IA) Policy/Guidance Manual, Version 1.3, February 2003
- DoD 5200.2-R, "Personnel Security ProgramDOD 5200.1-R Information Security ProgramDoD Information Technology Standards Registry (DISRMHS Enterprise Architecture
- DoD 8510.1-M, DoD Information Technology Security Certification and Accreditation Process (DITSCAP) Application Manual
- Defense Information Infrastructure (DII) Common Operating Environment (COE) Integration and Runtime Specification (I&RTS), Version 4.0, dated 4 October 99, and subsequent updates
- DoD 5400.11-R, DoD Privacy Program
- DoD Directive 8500.1, "Information Assurance (IA)" current version
- DoD Instruction 8500.2, "Information Assurance (IA) Implementation"
- DoD 6025.18-R, "DoD Health Information Privacy Regulation"
  DoD Instruction 8551.1, "Ports, Protocols, and Services Management"
- Clinger-Cohen Act of 1996, 40 U.S.C. 1401 et seq.
- DoD Instruction 8580.1, "Information Assurance (IA) in the Defense Acquisition System"
- DOD Architecture Framework Version 1.0, February 9, 2004
- CJCSI 3170.01E Joint Capabilities Integration and Development System, May 11, 2005
-

8.0 OTHER CLAUSES INCORPORATED INTO THIS TASK ORDER

8.1 FAR Clauses: The following FAR clauses are in addition to those covered in the GSA IT 70 Schedule Contract:

- **Organizational Conflict of Interest (FAR 9.5)**
- **FAR 52.204-9 - Personal Identity Verification of Contractor Personnel. (Jan 2011).**
- **FAR 52.217-5 - Evaluation of Options (Jul 1990)**
- **FAR 52.224-1 - Privacy Act Notification (Apr 1984)**
- **FAR 52.224-2 - Privacy Act (Apr 1984).**
- **FAR 52.227-14 - Rights in Data General (Dec 2007)**
- **FAR 52.232-18 - Availability of Funds (Apr 1984)**
- **FAR 52.232-25 - Prompt Payment**
- **FAR 52.222-54 - Employment Eligibility Verification (Jan 2009)**
- **FAR 52.227-16 - Additional Data Requirements (June 1987)**
- **FAR 52.232-19 - Availability of Funds for Next Fiscal Year (Apr 1984)**
- **FAR 52.239-1 - Privacy or Security Safeguards (Jul 2002)**
- **FAR 52.245-1 - Government Property (Aug 2010)**
- **FAR 52.246-4 - Inspection of Services – Fixed-Price (Aug 1996)**

- **FAR 52.217-8 Option to Extend Services (NOV 1999)** - The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed six (6) months. The Contracting Officer may exercise the option by written notice to the contractor within 30 calendar days of the end of

the task order period of performance.

- **FAR 52.217-9 - Option to Extend the Term of the Contract (Mar 2000)** - The government may extend the term of this contract by written notice to the contractor within thirty (30) calendar days before the contract expires; provided that the government gives the contractor a preliminary written notice of its intent to extend at least sixty (60) calendar days before the contract expires. The preliminary notice does not commit the government to an extension. If the government exercises this option, the extended contract shall be considered to include this option clause. The total duration of this contract, including the exercise of any options under this clause, shall not exceed five (5) years.

- **FAR 52.237-3 Continuity of Services (JAN 1991)**

(a) The contractor recognizes that the services under this contract are vital to the Government and must be continued without interruption and that, upon contract expiration, a successor, either the Government or another contractor, may continue them. The contractor agrees to—

(1) Furnish phase-in training; and

(2) Exercise its best efforts and cooperation to effect an orderly and efficient transition to a successor.

(b) The contractor shall, upon the Contracting Officer's written notice, (1) furnish phase-in, phase-out services for up to 90 calendar days after this contract expires and (2) negotiate in good faith a plan with a successor to determine the nature and extent of phase-in, phase-out services required. The plan shall specify a training program and a date for transferring responsibilities for each division of work described in the plan, and shall be subject to the Contracting Officer's approval. The contractor shall provide sufficient experienced personnel during the phase-in, phase-out period to ensure that the services called for by this contract are maintained at the required level of proficiency.

(c) The contractor shall allow as many personnel as practicable to remain on the job to help the successor maintain the continuity and consistency of the services required by this contract. The contractor also shall disclose necessary personnel records and allow the successor to conduct on-site interviews with these employees. If selected employees are agreeable to the change, the contractor shall release them at a mutually agreeable date and negotiate transfer of their earned fringe benefits to the successor.

(d) The contractor shall be reimbursed for all reasonable phase-in, phase-out costs (*i.e.,* costs incurred within the agreed period after contract expiration that result from phase-in, phase-out operations) and a fee (profit) not to exceed a pro rata portion of the fee (profit) under this contract.

- **FAR 52.219-6 Notice of Total Small Business Set-Aside**

As prescribed in 19.508(c), insert the following clause:

Notice of Total Small Business Set-Aside (Nov 2011)

(a) Definition. "Small business concern," as used in this clause, means a concern, including its affiliates that is independently owned and operated, not dominant in the field of operation in which it is bidding on Government contracts, and qualified as a small business under the size standards in this solicitation.

(b) Applicability. This clause applies only to--

(1) Contracts that have been totally set aside or reserved for small business concerns; and

(2) Orders set aside for small business concerns under multiple-award contracts as described in 8.405-5 and 16.505(b)(2)(i)(F).*

(c) General.
(1) Offers are solicited only from small business concerns. Offers received from concerns that are not small business concerns shall be considered nonresponsive and will be rejected.
(2) Any award resulting from this solicitation will be made to a small business concern.

(d) Agreement. A small business concern submitting an offer in its own name shall furnish, in performing the contract, only end items manufactured or produced by small business concerns in the United States or its outlying areas. If this procurement is processed under simplified acquisition procedures and the total amount of this contract does not exceed $25,000, a small business concern may furnish the product of any domestic firm. This paragraph does not apply to construction or service contracts.

- **FAR 52.219-28 – Post-Award Small Business Program Rerepresentation**

As prescribed in 19.309(c), insert the following clause:

Post-Award Small Business Program Rerepresentation (Jul 2013)

(a) Definitions. As used in this clause--

Long-term contract means a contract of more than five years in duration, including options. However, the term does not include contracts that exceed five years in duration because the period of performance has been extended for a cumulative period not to exceed six months under the clause at 52.217-8, Option to Extend Services, or other appropriate authority.

Small business concern means a concern, including its affiliates that is independently owned and operated, not dominant in the field of operation in which it is bidding on Government contracts, and qualified as a small business under the criteria in 13 CFR part 121 and the size standard in paragraph (c) of this clause. Such a concern is "not dominant in its field of operation" when it does not exercise a controlling or major influence on a national basis in a kind of business activity in which a number of business concerns are primarily engaged. In determining whether dominance exists, consideration shall be given to all appropriate factors, including volume of business, number of employees, financial resources, competitive status or position, ownership or control of materials, processes, patents, license agreements, facilities, sales territory, and nature of business activity.

(b) If the Contractor represented that it was a small business concern prior to award of this contract, the Contractor shall re-represent its size status according to paragraph (e) of this clause or, if applicable, paragraph (g) of this clause, upon the occurrence of any of the following:

(1) Within 30 calendar days after execution of a novation agreement or within 30 calendar days after modification of the contract to include this clause, if the novation agreement was executed prior to inclusion of this clause in the contract.

(2) Within 30 calendar days after a merger or acquisition that does not require a novation or within 30 calendar days after modification of the contract to include this clause, if the merger or acquisition occurred prior to inclusion of this clause in the contract.

(3) For long-term contracts—

(i) Within 60 to 120 calendar days prior to the end of the fifth year of the contract; and

(ii) Within 60 to 120 calendar days prior to the date specified in the contract for exercising any option thereafter.

(c) The Contractor shall re-represent its size status in accordance with the size standard in effect at the time of this re-representation that corresponds to the North American Industry Classification System (NAICS) code assigned to this contract. The small business size standard corresponding to this NAICS code can be found at http://www.sba.gov/content/table-small-business-size-standards .

(d) The small business size standard for a Contractor providing a product which it does not manufacture itself, for a contract other than a construction or service contract, is 500 employees.

(e) Except as provided in paragraph (g) of this clause, the Contractor shall make the representation required by paragraph (b) of this clause by validating or updating all its representations in the Representations and Certifications section of the System for Award Management (SAM) and its other data in SAM, as necessary, to ensure that they reflect the Contractor's current status. The Contractor shall notify the contracting office in writing within the timeframes specified in paragraph (b) of this clause that the data have been validated or updated, and provide the date of the validation or update.

(f) If the Contractor represented that it was other than a small business concern prior to award of this contract, the Contractor may, but is not required to, take the actions required by paragraphs (e) or (g) of this clause.

(g) If the Contractor does not have representations and certifications in SAM, or does not have a representation in SAM for the NAICS code applicable to this contract, the Contractor is required to complete the following re-representation and submit it to the contracting office, along with the contract number and the date on which the re-representation was completed:

The Contractor represents that it [ ] is, [ ] is not a small business concern under NAICS Code _____ assigned to contract number _____.[Contractor to sign and date and insert authorized signer's name and title].

8.2 DFARS Clauses: The following DFARS clauses are in addition to those covered in the GSA IT 70 Schedule Contract:

- **DFARS 252.227-7013 - Rights in Technical Data - Noncommercial Items (Nov 1995)**
- **DFARS 252.227-7014 - Rights in Noncommercial Computer - Software and Noncommercial Computer Software Documentation (Jun 1995)**
- **DFARS 252.227-7015 - Technical Data – Commercial Items (JUN 2013)**
- **DFARS 252.209-7999 - Representation By Corporations Regarding An Unpaid Delinquent Tax Liability Or A Felony Conviction Under Any Federal Law (DEVIATION 2014-00009) (FEB 2014).**

- **DFARS 252.232-7007 - LIMITATION OF GOVERNMENT'S OBLIGATION (MAY 2006)**

(a) Contract line item(s) * through * are incrementally funded. For these item(s), the sum of $ * of the total price is presently available for payment and allotted to this contract. An allotment schedule is set forth in paragraph (j) of this clause.

(b) For item(s) identified in paragraph (a) of this clause, the Contractor agrees to perform up to the point at which the total amount payable by the Government, including reimbursement in the event of termination of those item(s) for the Government's convenience, approximates the total amount currently allotted to the contract. The Contractor is not authorized to continue work on those item(s) beyond that point. The Government will not be obligated in any event to reimburse the Contractor in excess of the amount allotted to the contract for those item(s) regardless of anything to the contrary in the clause entitled "Termination for Convenience of the Government." As used in this clause, the total amount payable by the Government in the event of termination of applicable contract line item(s) for convenience includes costs, profit, and estimated termination settlement costs for those item(s).

(c) Notwithstanding the dates specified in the allotment schedule in paragraph (j) of this clause, the Contractor will notify the Contracting Officer in writing at least ninety (90) calendar days prior to the date when, in the Contractor's best judgment, the work will reach the point at which the total amount payable by the Government, including any cost for termination for convenience, will approximate 85 percent of the total amount then allotted to the contract for performance of the applicable item(s). The notification will state (1) the estimated date when that point will be reached and (2) an estimate of additional funding, if any, needed to continue performance of applicable line items up to the next scheduled date for allotment of funds identified in paragraph (j) of this clause, or to a mutually agreed upon substitute date. The notification will also advise the Contracting Officer of the estimated amount of additional funds that will be required for the timely performance of the item(s) funded pursuant to this clause, for a subsequent period as may be specified in the allotment schedule in paragraph (j) of this clause or otherwise agreed to by the parties. If after such notification additional funds are not allotted by the date identified in the Contractor's notification, or by an agreed substitute date, the Contracting Officer will terminate any item(s) for which additional funds have not been allotted, pursuant to the clause of this contract entitled "Termination for Convenience of the Government."

(d) When additional funds are allotted for continued performance of the contract line item(s) identified in paragraph (a) of this clause, the parties will agree as to the period of contract performance which will be covered by the funds. The provisions of paragraphs (b) through (d) of this clause will apply in like manner to the additional allotted funds and agreed substitute date, and the contract will be modified accordingly.

(e) If, solely by reason of failure of the Government to allot additional funds, by the dates indicated below, in amounts sufficient for timely performance of the contract line item(s) identified in paragraph (a) of this clause, the Contractor incurs additional costs or is delayed in the performance of the work under this contract and if additional funds are allotted, an equitable adjustment will be made in the price or prices (including appropriate target, billing, and ceiling prices where applicable) of the item(s), or in the time of delivery, or both. Failure to agree to any such equitable adjustment hereunder will be a dispute concerning a question of fact within the meaning of the clause entitled "Disputes."

(f) The Government may at any time prior to termination allot additional funds for the performance of the contract line item(s) identified in paragraph (a) of this clause.

(g) The termination provisions of this clause do not limit the rights of the Government under the clause entitled "Default." The provisions of this clause are limited to the work and allotment of funds for the contract line item(s) set forth in paragraph (a) of this clause. This clause no longer applies

once the contract is fully funded except with regard to the rights or obligations of the parties concerning equitable adjustments negotiated under paragraphs (d) and (e) of this clause.

(h) Nothing in this clause affects the right of the Government to terminate this contract pursuant to the clause of this contract entitled "Termination for Convenience of the Government."

(i) Nothing in this clause shall be construed as authorization of voluntary services whose acceptance is otherwise prohibited under 31 U.S.C. 1342.

(j) The parties contemplate that the Government will allot funds to this contract in accordance with the following schedule:

On execution of contract	$ _____
(Month) (Day), (Year)	$ _____
(Month) (Day), (Year)	$ _____
(Month) (Day), (Year)	$ _____

-End of Clause-

EXHIBIT 1: GLOSSARY OF ACRONYMS

ACRONYM	MEANING
AM	Acquisition Manager
API	Application Program Interfaces
AQL	Acceptable Quality Level
CAP	Contractor-Acquired-Government Owned Property
CASE	Computer-Aided Software Engineering
CDR	Contract Discrepancy Report
CDR	Critical Design Review
CFSR	Contract Funds Status Reports
CM	Configuration Management
CMM	Capability Maturity Model
COD-FC	Contract Operations Division - Falls Church
COR	Contracting Officer's Representative
COTS	Commercial Off-The-Shelf
CPARS	Contractor Performance Assessment Reporting System
CPFF	Cost Plus Fixed Fee
CS	Contract Specialist
CSC	Computer Software Components
CSCI	Computer Software Configuration Items
DA	Days after
DACA	Days after contract award (award of this order)
DAEOM	Days after end of month
Days	Calendar days, unless otherwise specified
DCAA	Defense Contract Audit Agency
DID	Data Item Description
DII COE	Defense Information Infrastructure/Common Operation Environment
DOA	Date of Award
DoD	Department of Defense
DT&E	Development, Test and Evaluation
E	Electronic Copy
EIT	Electronic and Information Technology
EVM	Earned Value Management
FAT	Factory Acceptance Tests
FFP	Firm Fixed Price
G&A	General and Administrative
GFE	Government Furnished Equipment
GFI	Government Furnished Information
GOTS	Government-Off-the-Shelf
GPO	Government Printing Office
GSA	U.S. General Services Administration
ID/IQ	Indefinite Delivery/Indefinite Quality
IEEE	Institute of Electrical and Electronics Engineers
IMP	Integrated Master Plan
IPPSRS	Integrated Program Planning, Scheduling, and Reporting System
IPT	Integrated Product/Process Team
JAC	Joint Application Configuration
JMIS	Joint Medical Information System
JTA	Joint Technical Architecture
KO	Contracting Officer
LPO	Local Processing Office

M&H	Material and Handling
MHS	Military Health System
MIS	Management Information Systems
MPR	Monthly Progress Report
NLT	Not Later Than
OCI	Organizational Conflict of Interest
ODC	Other Direct Costs
OT&E	Operation Test and Evaluation
PDR	Preliminary Design Review
PHI	Protected Health Information
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
POC	Point of Contact
PPBE	Planning, Programming, Budgeting and Execution
PR	Production Review
PWS	Performance Work Statement
PWS Ref	Performance Work Statement Reference (paragraph number)
QASP	Quality Assurance Surveillance Plan
QCP	Quality Control Plan
RM&A	Reliability, Maintainability, and Availability
ROI	Return on Investment
RTM	Requirements Traceability Matrix
SDD	Solutions Delivery Division
SEI	Software Engineering Institute
SME	Subject Matter Expert
SOO	Statement of Objectives
SOW	Statement of Work
SSR	System Specification Review
T&M	Time and Materials
TEAMS	TRICARE Evaluation, Analysis, and Management Support
TEPP	Test Evaluation Program Plan
TM	Task Manager
TMA	TRICARE Management Activity
TOPR	Task Order Proposal Request
TRR	Test Readiness Review
USAMRAA	U.S. Army Medical Research Acquisition Activity
WAWF	Wide Area Work Flow
WBS	Work Breakdown Structure
WDA	Working Days After